Guidelines for Safety Management of Medical Information by Providers of Information Systems and Services Handling Medical Information

Handbook for Google Cloud and Google Workspace

This document provides an overview of the security management measures implemented by Google Cloud and Google Workspace as a part of the information disclosure requirement under “The Safety Management Guideline for Information Systems and Service Providers Handling Medical Information” required by the Ministry of Economy, Trade, and Industry and the Ministry of Internal Affairs and Communications as of August 2020. Google's controls described in this document are certified by the third-party audit compliance programs ISO / IEC 27001, ISO / IEC 27017, and ISO / IEC 27018.
Since the "information flow" required by the "The Safety Management Guideline for Information Systems and Service Providers Handling Medical Information" differs for each user of Google Cloud and Google Workspace, it is difficult to present the response for each situation. Therefore, Google has released "Google’s Controls" regarding the items described in "Attachment 2 Correspondence Table between The List of Security Measures in The Old Guideline and The Guidelines for Safety Management of Medical Information".
* Each column, other than the row number, Google’s Controls, and ISO standard details, is based on the column structure of "Attachment 2 Correspondence Table between The List of Security Measures in The Old Guideline and The Guidelines for Safety Management of Medical Information".

Line	Measures	Category	Sub-Category	No.	Content of the requirements	Response of Google	Relevant ISO standards
1	1. Human and organizational measures	1.1. Provision of standards and manuals	①Provision of Access management standard	①-1	Create access control regulations which defines access restriction ,recording, and monitoring for the medical information systems.Provide the documentations in response to requests from medical institutions.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer’s data from that of other customers and users, even when it’s stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google’s internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google’s security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee’s authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and Google Workspace products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	· ISO 27001 2013, Annex A.9
2	1. Human and organizatio	1.1. Provision of standard	①Provision of Access managem	①-2	The access control regulations include the following: ・Access rights, registration application, change application, disposal application, and approval of them	Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27001:2013, Annex A.5) and Organization of Information Security (ISO27001:2013, Annex A.6).	· ISO 27001 2013, Annex A.5,6

	nal measures	s and manuals	ent standard		in the account management, regular verification process ・Storage and collection of the records for access and authentication, etc. ・Periodic review on the records for access and authentication, etc. ・Periodic review on the operational status of access control	Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	
3	1. Human and organizational measures	1.1. Provision of standards and manuals	②Provision of measures for connection of carried out device to external network	②-1	Include connection conditions for connecting to external networks and safety grip actions when the devices are taken out (Specific measures to prevent leakage or tampering of stored data (anti-malware measures, encryption, implementation of firewalls, etc.)) in operation management rules.	Google is certified to the ISO27001 Standard, which regulates "Documented Operating Procedures" (ISO27001:2013, Annex A.12.1.1). Google maintains robust internal documentation and maintains an ISMS, per ISO27001 requirements. All documentation in on systems that are replicated and subject to backup. Customers using Google Cloud Platform, retain all rights and responsibilities to configure and manage their environment, including development of operational guidance.	· ISO 27001 2013, Annex A.12.1.1
4	1. Human and organizational measures	1.1. Provision of standards and manuals	③Deletion of data	③-1	Provide the disposal procedures for CD-R and others.	Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2) and "Secure disposal or reuse of equipment" (ISO 27001:2013,Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.	· ISO 27001 2013, Annex A.8.3.2,11.2
5	1. Human and organizational measures	1.1. Provision of standards and manuals	③Deletion of data	③-2	Provide the disposal procedures for hard disk and others.	Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" (ISO 27001:2013,Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that	· ISO 27001 2013, Annex A.8.3.2,11.2.7

						the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.	
6	1. Human and organizational measures	1.1. Provision of standards and manuals	③Deletion of data	③-3	Include irreversible destruction, deletion and other measures to prevent restoration of original data in the discarding procedures.	Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" (ISO 27001:2013,Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.	· ISO 27001 2013, Annex A.8.3.2,11.2.7
7	1. Human and organizational measures	1.1. Provision of standards and manuals	③Deletion of data	③-4	When a hard disk or the like is reused by another device in the medical information system, erase the data by a reliable method such as erasing the original data by writing the data a plurality of times before reusing the hard disk or the like, and confirm that the information is erased before reuse.	Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" ((ISO 27001:2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" ((ISO 27001:2013,Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.	· ISO 27001 2013, Annex A.8.3.2,11.2.7
8	1. Human and organizational measures	1.1. Provision of standards and manuals	③Deletion of data	③-5	If passwords for hardware such as BIOS passwords and hard disk passwords for servers are set, delete the passwords.	Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" ((ISO 27001:2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" ((ISO 27001:2013,Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors	· ISO 27001 2013, Annex A.8.3.2,11.2.7

						and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. Google follows the Clear method recommended by NIST SP 800-88 Rev. 1 "Guidelines for Media Sanitization", Appendix A. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.	
9	1. Human and organizational measures	1.1. Provision of standards and manuals	③Deletion of data	③-6	When connecting a hard disk to a device, whether it is reused or not, verify that an unauthorized program or the like is not recorded in the device for verification.	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001:2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/.	· ISO 27001 2013, Annex A.8.3.2,11.2.7
10	1. Human and organizational measures	1.1. Provision of standards and manuals	③Deletion of data	③-7	For discarding hard disks, apply erasure of original data by writing data a plurality of times, measures for erasing the original data by strong magnetic, physical destruction measures (such as melting and cutting by high temperature), etc. to prevent reuse and readout of data. Maintain records of outlines of measures performed on the machineries (the format of the target devices, management numbers, workers in charge of work, date and time of work, content of work, etc.) so that they can be submitted promptly in response to requests from healthcare institutions, etc.	Information security oversight and management controls, including Storage Media Security controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google utilizes barcodes and asset tags to track the status and location of data center equipment from acquisition to installation, retirement, and destruction. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. Google hard drives leverage technologies, like Full Disk Encryption (FDE) and drive locking, to protect data at rest. Personable Identifiable Information (PII) on removable media leaving Google facilities is approved and encrypted. When a hard drive is retired, authorized individuals verify that the disk is erased by writing zeros to the drive and performing a multiple-step verification process to help ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multistage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.	-

						Google employs a static fully automated workflow tool to review, approve and track disks through the sanitization and destruction process.	
11	1. Human and organizational measures	1.1. Provision of standards and manuals	③Deletion of data	③-8	Physical destruction measures should be taken by the information processing provider itself. However, when requesting external businesses, the rationale for selection of providers should be given to medical institutions, etc. and approval of outsourcing should be obtained.Receive and store a certificate or the like indicating that information cannot be read due to destructive actions. The reliable methods of hard disk disposal is irradiating certain level of magnetic field line or physically destroying the hard disk by melting process or in other ways. However, data erasure methods performed by softwares which write random data and fixed patterns multiple times (such as NSA recommended method, US Department of Defense compliant method, NATO method, Gutmann method and others), are also commonly used.	Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" ((ISO 27001:2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" ((ISO 27001:2013,Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.	· ISO 27001 2013, Annex A.8.3.2,11.2.7
12	1. Human and organizational measures	1.1. Provision of standards and manuals	③Deletion of data	③-9	When discarding electronic media, apply physical destructive actions (such as high-temperature fusing and cutting) to ensure that the information cannot be read.	Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" ((ISO 27001:2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" ((ISO 27001:2013,Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.	· ISO 27001 2013, Annex A.8.3.2,11.2.7
13	1. Human and organizational measures	1.1. Provision of standards and manuals	③Deletion of data	③-10	The operational grip rules are as follows: ・ The necessity of providing medical information systems should be periodically checked for the personal data to be grip or the medium in which it is stored.	Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" (ISO 27001:2013,Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it	· ISO 27001 2013, Annex A.8.3.2,11.2.7

					・ The procedures for discarding the personal data and the medium in which it is stored, which are not required for the provision of medical information systems. ・ When discarding the personal data which is not necessary for providing medical information systems and the medium in which it is stored, actions are taken to prevent the subject from suffering unexpected damage (for example, notifying the discarding standard in advance).	is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.	
14	1. Human and organizational measures	1.1. Provision of standards and manuals	③Deletion of data	③-11	Agree with medical institutions about the procedures for destroying information.	Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" (ISO 27001:2013,Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.	· ISO 27001 2013, Annex A.8.3.2,11.2.7
15	1. Human and organizational measures	1.1. Provision of standards and manuals	④Measures for carry out of data and devices out of office	④-1	Provide that the personal data to be consigned is not stored in the terminal used for operation and maintenance in the operation grip regulations of the company, etc.	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A.11.2). Google’s focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers	· ISO 27001 2013, Annex A.8.1,8.3.2,11.2.7,12.5

16	1. Human and organizational measures	1.1. Provision of standards and manuals	④Measures for carry out of data and devices out of office	④-2	When it is necessary to bring a device or the like storing medical information outside the organization of a medical institution or a cloud service provider (including a subcontractor) for the purpose of maintenance (for example, repair of the device), the procedure should be formulated.	Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" (ISO 27001:2013,Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.	· ISO 27001 2013, Annex A.8.3.2,11.2.7
17	1. Human and organizational measures	1.1. Provision of standards and manuals	④Measures for carry out of data and devices out of office	④-3	Agree with medical institutions on the procedures and information provision conditions specified in ④-2.	Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" (ISO 27001:2013,Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.	· ISO 27001 2013, Annex A.8.3.2,11.2.7
18	1. Human and organizational measures	1.1. Provision of standards and manuals	④Measures for carry out of data and devices out of office	④-4	Develop appropriate verification procedures to reinstall the removed equipment.	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001:2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher	· ISO 27001 2013, Annex A.8.1,8.3.2,11.2.7,12.5

						that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	
19	1. Human and organizational measures	1.1. Provision of standards and manuals	④Measures for carry out of data and devices out of office	④-5	When a troubleshooting external is performed when a disability or the like is found in the maintenance and inspection, the operation should be performed in an area management to the information processing provider, so that the troubleshooting operation is not carried out to the outside. When it is necessary to carry out an operation to the outside, the electro-magnetic recording in the device should be erased without fail and then taken out. For a device such as a storage device whose information cannot be erased due to a disability, select discard after performing physical destruction instead of repair.	Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" ((ISO 27001:2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" ((ISO 27001:2013,Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.	· ISO 27001 2013, Annex A.8.3.2,11.2.7
20	1. Human and organizational measures	1.1. Provision of standards and manuals	④Measures for carry out of data and devices out of office	④-6	The following items can be considered as items included in the taking-out procedure. ・ Format of the application form for taking out the machinery (applicant information, approver information, object equipment information, take-out date and time, scheduled return date and time, information on place of taking out, reason of taking out, outline of information stored in the equipment, result of risk evaluation due to taking out, countermeasure in case the equipment is lost or damaged) ・ Request approval process ・ Return confirmation process, etc.	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001:2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	· ISO 27001 2013, Annex A.8.1,8.3.2,11.2.7,12.5

Guidelines for Safety Management of Medical Information by Providers of Information Systems and Services Handling Medical Information

Handbook for Google Cloud and Google Workspace

21	1. Human and organizational measures	1.1. Provision of standards and manuals	④Measures for carry out of data and devices out of office	④-7	The following items may be included in the verification procedure at the time of return. ・ Checking machine operation ・ Whether or not there is a device that threatens the security of information, such as an eavesdropping device. ・ Detection of malicious programs ・ Verification of stored information (unauthorized tampering, etc.), etc.	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001:2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	· ISO 27001 2013, Annex A.8.1,8.3.2,11.2.7,12.5
22	1. Human and organizational measures	1.1. Provision of standards and manuals	⑤Provision of management manual for carried out devices and elements	⑤-1	Policies and rules related to the removal (including removal from the consignor) of equipments and media that store information related to services (consignment information, information related to information systems, etc.) shall be defined in the Operation grip Rules.	Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" (ISO 27001:2013,Annex A.11.2.7), and "Cryptography" (ISO 27001:2013, Annex A.10). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. Please see https://cloud.google.com/security/encryption-in-transit/ for more informaiton.	· ISO 27001 2013, Annex A.8.3.2,11.2.7,10
23	1. Human and organizatio	1.1. Provision of	⑤Provision of managem	⑤-2	The term "take-out" in ⑤-1 includes not only physical taking-out but also send to the outside through a network.	Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" (ISO 27001:2013,Annex A.11.2.7), and "Cryptography" (ISO 27001:2013, Annex A.10).	· ISO 27001 2013, Annex A.8.3.2,11.2.7,10

	nal measures	standards and manuals	ent manual for carried out devices and elements			Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. Please see https://cloud.google.com/security/encryption-in-transit/ for more informaiton.	
24	1. Human and organizational measures	1.1. Provision of standards and manuals	⑤Provision of management manual for carried out devices and elements	⑤-3	Agree with medical institutions, etc. for the contents defined in ⑤-1.	Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" (ISO 27001:2013,Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.	· ISO 27001 2013, Annex A.8.3.2,11.2.7
25	1. Human and organizational measures	1.1. Provision of standards and manuals	⑤Provision of management manual for carried out devices and elements	⑤-4	Do not unnecessarily take electronic media out of information processing business facilities. For electronic media such as CDs, DVDs, MOs and others, use optical media that cannot be additionally written (such as CD-R, DVDR and others.), and reliably dispose the electronic media after the completion of the data exchanging operation.	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A.11.2), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" (ISO 27001:2013,Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure	· ISO 27001 2013, Annex A.11.2, 8.3.2, 11.2.7

						the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.	
26	1. Human and organizational measures	1.1. Provision of standards and manuals	⑤Provision of management manual for carried out devices and elements	⑤-5	When large-capacity electronic media such as MTs, DATs, solid state memory devices, and hard disks are used for data interchange and back-up purposes, strict management should be made. When information is recorded on these electronic media a plurality of times, measures against information leakage such as reliable information erasure should be taken instead of simply overwriting.	Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" ((ISO 27001:2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" ((ISO 27001:2013,Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.	· ISO 27001 2013, Annex A.8.3.2,11.2.7
27	1. Human and organizational measures	1.1. Provision of standards and manuals	⑤Provision of management manual for carried out devices and elements	⑤-6	All electronic media should be labeled to indicate the level of confidentiality of the information being stored.	Google is certified to the ISO27001 Standard, which regulates "Information classification" (ISO 27001:2013, Annex A.8.2). Information security oversight and management controls, including software development controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers can apply their own data-labeling standard to information stored in Google Cloud.	· ISO 27001 2013, Annex A.8.2
28	1. Human and organizational measures	1.1. Provision of standards and manuals	⑤Provision of management manual for carried out devices and elements	⑤-7	For recording media and recording equipment used for services, include the following in the Operation grip Rules. ・ Grip System and grip Methods ・ Treatment of Recording Media and Recording Devices ・ Policies and rules related to the removal (including removal from the consignor) of equipments and media that store information related to services (consignment information, information related to information systems, etc.) (In addition to physical removal, "removal" includes transmission to the outside via a network).	Google is certified to the ISO27001 Standard, which regulates "Documented Operating Procedures" (ISO27001:2013, Annex A.12.1.1). Google maintains robust internal documentation and maintains an ISMS, per ISO27001 requirements. All documentation in on systems that are replicated and subject to backup. Customers using Google Cloud Platform, retain all rights and responsibilities to configure and manage their environment, including development of operational guidance.	· ISO 27001 2013, Annex A.12.1.1

					・ When information on services is taken out, the equipment and media that store the information are stolen or lost (in addition to physical theft or loss of equipment and media at the time of take-out, system grip is sent to the outside that is not approved by the system operator (including malicious responses by third parties, erroneous transmissions by employees, etc.))		
29	1. Human and organizational measures	1.1. Provision of standards and manuals	⑤Provision of management manual for carried out devices and elements	⑤-8	Educate employees about the contents described in ⑤-7.	Google is certified to the ISO27001 Standard, which regulates "Information Security Awareness, Education and Training" (ISO 27001:2013, Annex A.7.2.2), Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All Google contractors undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new contractors agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.	· ISO 27001 2013, Annex A.7.2.2
30	1. Human and organizational measures	1.1. Provision of standards and manuals	⑤Provision of management manual for carried out devices and elements	⑤-9	Compliance with the operation grip regulations described in ⑤-7 is also required for the subcontractor.	Google is certified to the ISO27001 Standard, which regulates "Information Security Awareness, Education and Training" (ISO 27001:2013, Annex A.7.2.2), Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All Google contractors undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new contractors agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.	· ISO 27001 2013, Annex A.7.2.2
31	1. Human and organizational measures	1.1. Provision of standards and manuals	⑥Provision of manual related to quality managem	⑥-1	Develop appropriate procedures for changing information processing apparatuses and software. Maintenance operations should be notified to medical institutions and approved in advance with sufficient room.	Google is certified to the ISO27001 Standard, which regulates "Change Management" (ISO27001:2013 Annex A 12.1.2) and "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14). Please see the Google Infrastructure Security Design Overview - https://cloud.google.com/security/security-design/ for more details.	· ISO 27001 2013, Annex A.12.1.2,14

			ent of device and software			Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including change management and system development procedures.	
32	1. Human and organizational measures	1.1. Provision of standards and manuals	⑥Provision of manual related to quality management of device and software	⑥-2	Include the measures and procedures related to the quality grip of the equipment and software in the operation grip regulations, etc.	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001:2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software" (ISO 27001:2013, Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	· ISO 27001 2013, Annex A.8.1,8.3.2,11.2.7,12.5
33	1. Human and organizational measures	1.1. Provision of standards and manuals	⑥Provision of manual related to quality management of device and software	⑥-3	Educate employees about the quality grip of equipment and software.	Google is certified to the ISO27001 Standard, which regulates "Information Security Awareness, Education and Training" (ISO 27001:2013, Annex A.7.2.2), Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All Google contractors undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new contractors agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.	· ISO 27001 2013, Annex A.8.1,8.3.2,11.2.7,12.5
34	1. Human and organizational measures	1.1. Provision of standard	⑥Provision of manual related to quality	⑥-4	Request the subcontractors related to medical information systems to respond with the provider's quality control, which aims to follow the requirements of this guideline.	Google is certified to the ISO27001 Standard, which regulates "Information Security Awareness, Education and Training" (ISO 27001:2013, Annex A.7.2.2), Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report.	· ISO 27001 2013, Annex A.8.1,8.3.2,11.2.7,12.5

		s and manuals	managem ent of device and software			All Google contractors undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new contractors agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.	
35	1. Human and organizatio nal measures	1.1. Provision of standard s and manuals	⑥Provisio n of manual related to quality managem ent of device and software	⑥-5	The change procedure may include the following items. ・ Process of notifying the affected parties about the change ・ Format of change application form of machinery (applicant information, approver information, object equipment information, change operation start date and time, change operation period, change reason, summary of information stored in equipment, risk evaluation result due to change, countermeasure in case of equipment damage, etc.) ・ Request approval process ・ Change testing process ・ Recovery procedure in case of trouble in the change work ・ Change end confirmation process ・ The process of monitoring the impact of changes, etc.	Google is certified to the ISO27001 Standard, which regulates "Change Management" (ISO27001:2013 Annex A 12.1.2) and "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14). Please see the Google Infrastructure Security Design Overview - https://cloud.google.com/security/security-design/ for more details. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including change management and system development procedures.	· ISO 27001 2013, Annex A.12.1.2,14
36	1. Human and organizatio nal measures	1.2. Use of testing data which does not include personal informati on	①Measur es for usage of data including personal informatio n	①-1	Do not use medical information directly as development and testing data. In the case of use, specify data operations such as deleting personal information and replacing some data with random data so that the original data cannot be restored. Indicate to the medical institution that sufficient safety is guaranteed, and use the data after understanding.	Google is certified to the ISO27001 Standard, which regulates "Separation of Development, Testing, and Operational Environments" (ISO 27001:2013, Annex A.12.1.4), " and Security in Development and Support Processes" (ISO 27001:2013, Annex A.14.2). Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	· ISO 27001 2013, Annex A.12.1.4,14.2
37	1. Human and organizatio nal measures	1.3. Contract related to confidenti ality obligation	①Contrac t engagem ent of confidenti ality obligation	①-1	For all information processing operator personnel who may manipulate medical information, the stealthy retention contract must be signed at the time of employment contract or as a condition for the task of handling medical information. Telecommunications employees should be selected and dispatched on the assumption that stealthy must	Google is certified to the ISO27001 Standard, which regulates ""Terms and Conditions of Employment"" (ISO 27001:2013, Annex A.7.1.2), Hiring practices controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google performs background checks on new hires as permitted by local laws	· ISO 27001 2013, Annex A.7.1.2

			with all staff for provision of medical information system		be retained and continuous information-security education must be imposed.		
38	1. Human and organizational measures	1.3. Contract related to confidentiality obligation	①Contract engagement of confidentiality obligation with all staff for provision of medical information system	①-2	For contractor staff (including temporary staff) who may manipulate medical information, the content of confidentiality obligations should be included in work rules or others.	Google Cloud and Google Workspace are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://workspace.google.com/terms/dpa_terms.html	-
39	1. Human and organizational measures	1.3. Contract related to confidentiality obligation	①Contract engagement of confidentiality obligation with all staff for provision of medical information system	①-3	Provide a ledger and return confirmation procedure beforehand in order to confirm that all information asset has completely returned when the staff(including temporary staff) of an information processing business operator who operates medical information leaves the office. It is also necessary to sign an agreement that states that medical information learned from work should be managed confidentially after retirement. For dispatch employees, request a signature on the same agreement at the time of termination of the dispatch contract.	Google is certified to the ISO27001 Standard, which regulates ""Terms and Conditions of Employment"" (ISO 27001:2013, Annex A.7.1.2), Hiring practices controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google performs background checks on new hires as permitted by local laws	· ISO 27001 2013, Annex A.7.1.2
40	1. Human and organizational measures	1.3. Contract related to confidentiality obligation	①Contract engagement of confidentiality obligation with all staff for provision	①-4	Employment contracts, dispatch contracts or work rules should include confidentiality obligations for personal data handled during the work, when the contractor staff (including temporary staff) operating the medical information leaves office.	Google is certified to the ISO27001 Standard, which regulates "Terms and Conditions of Employment" (ISO 27001:2013, Annex A.7.1.2), Hiring practices controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google performs background checks on new hires as permitted by local laws	· ISO 27001 2013, Annex A.7.1.2

			of medical information system				
41	1. Human and organizational measures	1.3. Contract related to confidentiality obligation	①Contract engagement of confidentiality obligation with all staff for provision of medical information system	①-5	Include appropriate penalties in employment contracts or dispatch contracts or in work rules, etc. for employees, dispatch operators, etc. who violate the above-mentioned. Inform each staff member of the specific content of the disciplinary procedure and confirm that each staff member understands it.	Google is certified to the ISO27001 Standard, which regulates "Terms and Conditions of Employment" (ISO 27001:2013, Annex A.7.1.2), Hiring practices controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report.	· ISO 27001 2013, Annex A.7.1.2
42	1. Human and organizational measures	1.3. Contract related to confidentiality obligation	①Contract engagement of confidentiality obligation with all staff for provision of medical information system	①-6	Agree with medical institutions to provide data on the status of education and training for personnel(including temporary staff) engaged in the provision of medical information, the status of responses to confidentiality obligations, etc.	Google is certified to the ISO27001 Standard, which regulates "Terms and Conditions of Employment" (ISO 27001:2013, Annex A.7.1.2), Hiring practices controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google performs background checks on new hires as permitted by local laws	· ISO 27001 2013, Annex A.7.1.2
43	1. Human and organizational measures	1.3. Contract related to confidentiality obligation	②Contract engagement including confidentiality obligations with medical institutions and	②-1	Include information on medical information systems and confidentiality obligations on commissioned information in medical information systems provision contracts. The contract includes the fact that a penalty is imposed on a contractor that violates the confidentiality obligation, and the contents related to the supervision by medical institutions and the like on the treatment of the consigned information.	Google Cloud and Google Workspace are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://workspace.google.com/terms/dpa_terms.html	-

			sub-contractors				
44	1. Human and organizational measures	1.3. Contract related to confidentiality obligation	②Contract engagement including confidentiality obligations with medical institutions and sub-contractors	②-2	Procedures including confirmation of operations by personnel and consignees for whom confidentiality obligations are imposed should be defined when data including consigned personal data is inevitably used for confirmation of operations of medical information systems.	Not applicable. This is the customer's responsibility to respond to.	-
45	1. Human and organizational measures	1.3. Contract related to confidentiality obligation	②Contract engagement including confidentiality obligations with medical institutions and sub-contractors	②-3	Agree with the medical institution when the commissioned personal data is unavoidably used in order to confirm the operation of the medical information system.	Not applicable. This is the customer's responsibility to respond to.	-
46	1. Human and organizational measures	1.4. Performance of education and training	①Performance of education and training related to provision of medical information system	①-1	Educate all information processing operators who may operate medical information about information security and only employees who have a certain level of understanding will be engaged in the work.	Google is certified to the ISO27001 Standard, which regulates "Information Security Awareness, Education and Training" (ISO 27001:2013, Annex A.7.2.2), Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All Google contractors undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new contractors agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations	· ISO 27001 2013, Annex A.7.2.2

						on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.	
47	1. Human and organizational measures	1.4. Performance of education and training	①Performance of education and training related to provision of medical information system	①-2	For dispatch employees, ask the dispatcher to select and dispatch personnel who have or can have a certain level of knowledge and understanding of information security. After acceptance, provide training equivalent to regular personnel.	Google is certified to the ISO27001 Standard, which regulates "Information Security Awareness, Education and Training" (ISO 27001:2013, Annex A.7.2.2), Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All Google contractors undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new contractors agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.	· ISO 27001 2013, Annex A.7.2.2
48	1. Human and organizational measures	1.4. Performance of education and training	①Performance of education and training related to provision of medical information system	①-3	This education should be conducted periodically according to new threats and changes in information security technology.	Google is certified to the ISO27001 Standard, which regulates "Information Security Awareness, Education and Training" (ISO 27001:2013, Annex A.7.2.2), Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All Google contractors undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new contractors agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.	· ISO 27001 2013, Annex A.7.2.2
49	1. Human and organizational measures	1.4. Performance of education and training	①Performance of education and training related to provision of medical information system	①-4	Education and Training should include the confidentiality obligations of personnel related to manipulation of medical information systems at the time of retirement or after the termination of the contract.	Google is certified to the ISO27001 Standard, which regulates "Terms and Conditions of Employment" (ISO 27001:2013, Annex A.7.1.2), Hiring practices controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google performs background checks on new hires as permitted by local laws	· ISO 27001 2013, Annex A.7.1.2
50	1. Human and	1.5. Monitorin	①Moniroing of	①-1	In the event of suspicion of violations of safety management measures by contractor staff, the right to	Google is certified to the ISO27001 Standard, which regulates "Access to Networks and Network Services" (ISO27001:2013, Annex A.9.1.2), "Network Controls" (ISO27001:2013, Annex A.13.1.1).	· ISO 27001 2013, Annex A.9.1.2,13.1

	organizational measures	g of operational status	inspection and manipulation of medical information system		access medical information must be immediately stopped and it should be verified that no action such as tampering or destruction has been performed.	We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately.	
51	1. Human and organizational measures	1.5. Monitoring of operational status	①Moniroing of inspection and manipulation of medical information system	①-2	When the maintenance work of the information system is performed, in principle, managers of medical institutions should be notified in advance and after the work by a document or in other ways. Agree with medical institutions on tasks that require prior understanding and how to deal with cases where prior understanding of the tasks cannot be obtained.	Google has published the Terms of Service which outlines contractual obligations and agreements. Google Cloud Platform - Terms of Service: https://cloud.google.com/terms/ Google Workspace - Terms of Service: https://workspace.google.com/terms/premier_terms.html Section "1.4 Modifications. (a) To the Services." mentions "Google may make commercially reasonable updates to the Services from time to time. Google will inform Customer if Google makes a material change to the Services that has a material impact on Customer's use of the Services provided that Customer has subscribed with Google to be informed about such change."	-
52	1. Human and organizational measures	1.5. Monitoring of operational status	①Moniroing of inspection and manipulation of medical information system	①-3	After the maintenance operation is performed, report the medical institutions, etc. and gain confirmation from the managers of medical institutions. Agree with medical institutions about this procedure.	Google has published the Terms of Service which outlines contractual obligations and agreements. Google Cloud Platform - Terms of Service: https://cloud.google.com/terms/ Google Workspace - Terms of Service: https://workspace.google.com/terms/premier_terms.html Section "1.4 Modifications. (a) To the Services." mentions "Google may make commercially reasonable updates to the Services from time to time. Google will inform Customer if Google makes a material change to the Services that has a material impact on Customer's use of the Services provided that Customer has subscribed with Google to be informed about such change."	-

53	1. Human and organizational measures	1.5. Monitoring of operational status	①Monitoring of inspection and manipulation of medical information system	①-4	Agree with medical facilities for the response when the maintenance work of the medical information systems is carried inside the institutions such as medical institutions.	Not applicable. This is the customer's responsibility to respond to.	-
54	1. Human and organizational measures	1.5. Monitoring of operational status	②Periodical confirmation of location of devices and elements	②-1	Create and management a register for electronic media. Periodically verify registers and electronic media to verify theft and loss. In the ledger, records should be made regarding the use of electronic media and maintained for a certain period of time after the disposal of electronic media.	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001:2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	· ISO 27001 2013, Annex A.8.1,8.3.2,11.2.7,12.5
55	1. Human and organizational measures	1.5. Monitoring of operational status	②Periodical confirmation of location of devices and elements	②-2	For devices and media that store information, perform register grip, etc. and periodically check the location of the devices and media.	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001:2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then	· ISO 27001 2013, Annex A.8.1,8.3.2,11.2.7,12.5

						recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	
56	1. Human and organizational measures	1.5. Monitoring of operational status	②Periodical confirmation of location of devices and elements	②-3	The equipment and media in which personal data is stored must be the minimum required for the provision and operation of services, and the location and inventory of the equipment and media must be periodically checked.	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A.11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers	· ISO 27001 2013, Annex A.8.1,8.3.2,11.2.7,12.5
57	1. Human and organizational measures	1.5. Monitoring of operational status	③Performance of internal audit regarding the system structure and operational status of software	③-1	Include the content, procedures, etc. of internal audits related to system configuration and software operation status in the operation grip regulations, etc.	Google is certified to the ISO27001 Standard, which regulates "Change Management" (ISO27001:2013 Annex A 12.1.2) and "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14). Please see the Google Infrastructure Security Design Overview - https://cloud.google.com/security/security-design/ for more details. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including change management and system development procedures.	· ISO 27001 2013, Annex A.12.1.2,14
58	1. Human and organizational measures	1.6. Measures for physical data transfer	①Measures for data to carry out such as encryption	①-1	The following measures should be taken when physically conveying information. ・ Choose a reliable carrier based on standards agreed upon by medical institutions, etc. ・ Identification of operators at the time of delivery should be checked at both the sender and receiver to prevent third-party spoofing.	Media used to store data will not be transferred outside of Google's data centers. If a customer of Google cloud is physically transporting media containing data, please respond to this item as part of the customer's responsibility.	-

					・ In order to prevent electronic media from being picked up by a distributor or the like, the number and type of electronic media to be exchanged must be exchanged in advance to confirm that there is no loss at the time of receipt. ・ To prevent information from being extracted from an electronic medium by a distributor or the like, a container or the like that can detect unauthorized opening should be used. ・ When electronic media is sent or received, it must be sent directly to the carrier and not through a third party. ・ When exchanging information via electronic media, the materials in the electronic media should be encrypted if there are risks in the safety management during the transfer of the data.		
59	1. Human and organizational measures	1.7. Restriction on analysis and provision to third party	① Restriction on analysis and provision of medical data to third party	①-1	It should be the minimum necessary to browse the commissioned medical information for maintenance and operation.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer’s data from that of other customers and users, even when it’s stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google’s internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google’s security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee’s authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and Google Workspace products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	· ISO 27001 2013, Annex A.9

60	1. Human and organizational measures	1.7. Restriction on analysis and provision to third party	① Restriction on analysis and provision of medical data to third party	①-2	Except in emergencies, if it is necessary to browse the system according to ①-1, it shall be approved in advance and after by the system grip operator.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and Google Workspace products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	· ISO 27001 2013, Annex A.9
61	1. Human and organizational measures	1.7. Restriction on analysis and provision to third party	① Restriction on analysis and provision of medical data to third party	①-3	When the commissioned medical information is browsed in an emergency, the extent of the commissioned medical information and the reason why the commissioned medical information must be browsed in an emergency are indicated and approved by the systems grip operator.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and Google Workspace products.	· ISO 27001 2013, Annex A.9

						Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	
62	1. Human and organizational measures	1.7. Restriction on analysis and provision to third party	① Restriction on analysis and provision of medical data to third party	①-4	Agree on the scope and procedures of the browsing in ①-1 to ①-3 with medical institutions, etc. In addition, when medical information is browsed according to ①-2 and ①-3, a report should be promptly sent to medical institutions.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and Google Workspace products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	· ISO 27001 2013, Annex A.9
63	1. Human and organizational measures	1.7. Restriction on analysis and provision to third party	① Restriction on analysis and provision of medical data to third party	①-5	The analysis and analysis of entrusted medical information is not performed except when entrusted by medical institutions based on contract independent of contract for service provision.	Not applicable. This is the customer's responsibility to respond to. Customer data will be always processed based on the contracted method. Google's Privacy Protection Responsibility: https://cloud.google.com/security/privacy/	-

64	1. Human and organizational measures	1.7. Restriction on analysis and provision to third party	① Restriction on analysis and provision of medical data to third party	①-6	The information obtained by anonymously processing the entrusted medical information is also handled according to the medical information.	Not applicable. This is the customer's responsibility to respond to. Customer data will be always processed based on the contracted method. Google's Privacy Protection Responsibility: https://cloud.google.com/security/privacy/	-
65	1. Human and organizational measures	1.7. Restriction on analysis and provision to third party	① Restriction on analysis and provision of medical data to third party	①-7	Submitted medical information shall not be provided to third parties, including the patient, except by law or on the basis of instructions from medical institutions.	Google Cloud and Google Workspace are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://workspace.google.com/terms/dpa_terms.html	-
66	1. Human and organizational measures	1.7. Restriction on analysis and provision to third party	① Restriction on analysis and provision of medical data to third party	①-8	Include the contents of ①-7 in the contract related to provision of medical information systems.	Google Cloud and Google Workspace are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://workspace.google.com/terms/dpa_terms.html	-
67	1. Human and organizational measures	1.7. Restriction on analysis and provision to third party	① Restriction on analysis and provision of medical data to third party	①-9	Provide measures to prevent access and acquisition of medical information by unauthorised personnel, when the provider is providing (browsing) the medical information to third-party under the instruction of medical institutions.	Not applicable. This is the customer's responsibility to respond to. Customer data will be always processed based on the contracted method. Google's Privacy Protection Responsibility: https://cloud.google.com/security/privacy/	-
68	1. Human and organizational measures	1.7. Restriction on analysis and provision	① Restriction on analysis and provision	①-10	In the case of providing (browsing) data to third party according to ①-9, the ID and access rights of the person who can browse and acquire the data should be promptly changed and deleted under the instructions of the medical institution or the person who	Not applicable. This is the customer's responsibility to respond to. Customer data will be always processed based on the contracted method. Google's Privacy Protection Responsibility: https://cloud.google.com/security/privacy/	-

		to third party	of medical data to third party		has received the consignment (medical information collaboration network, etc.).		
69	1. Human and organizational measures	1.7. Restriction on analysis and provision to third party	① Restriction on analysis and provision of medical data to third party	①-11	When a third party is provided with medical information entrusted based on instructions from medical institutions, the contents (provider (viewer), browsing information, browsing date and time, etc.) shall be reported to medical institutions.	Not applicable. This is the customer's responsibility to respond to. Customer data will be always processed based on the contracted method. Google's Privacy Protection Responsibility: https://cloud.google.com/security/privacy/	-
70	1. Human and organizational measures	1.7. Restriction on analysis and provision to third party	① Restriction on analysis and provision of medical data to third party	①-12	Agree with medical institutions on terms and ranges for providing information to third parties and reporting according to ①-7 to ①-11.	Not applicable. This is the customer's responsibility to respond to. Customer data will be always processed based on the contracted method. Google's Privacy Protection Responsibility: https://cloud.google.com/security/privacy/	-
71	1. Human and organizational measures	1.8. Provision of records for data deletion	①Aquire of performance records for data deletion and provision of it to medical institutions	①-1	When information is discarded, in response to a request from a medical institution, report the implementation details including the person in charge of implementation and the method of deleting the information (such as demagnetization and physical destruction of an electro-magnetic recording medium) to the medical institution, and submit the discard record.	Information security oversight and management controls, including Storage Media Security controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google utilizes barcodes and asset tags to track the status and location of data center equipment from acquisition to installation, retirement, and destruction. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. Google hard drives leverage technologies, like Full Disk Encryption (FDE) and drive locking, to protect data at rest. Personable Identifiable Information (PII) on removable media leaving Google facilities is approved and encrypted. When a hard drive is retired, authorized individuals verify that the disk is erased by writing zeros to the drive and performing a multiple-step verification process to help ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multistage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Google employs a static fully automated workflow tool to review, approve and track disks through the sanitization and destruction process.	-

72	1. Human and organizational measures	1.8. Provision of records for data deletion	①Aquire of performance records for data deletion and provision of it to medical institutions	①-2	Physical destruction measures should be taken by the information processing provider itself. However, when requesting external businesses, the rationale for selection of providers should be given to medical institutions, etc. and understanding should be obtained. Receive and store a certificate or the like indicating that information cannot be read due to destructive actions.	Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" (ISO 27001:2013,Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.	· ISO 27001 2013, Annex A.8.3.2,11.2.7
73	1. Human and organizational measures	1.8. Provision of records for data deletion	①Aquire of performance records for data deletion and provision of it to medical institutions	①-3	Agree with medical institutions on the measures to be taken in ①-1 and the conditions necessary to provide the data.	Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" (ISO 27001:2013,Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Please see Google's Terms of Service, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://workspace.google.com/terms/dpa_terms.html	· ISO 27001 2013, Annex A.8.3.2,11.2.7
74	1. Human and organizational measures	1.8. Provision of records for data deletion	①Aquire of performance records for data deletion and	①-4	When the service of medical information system has stopped or medical institutions have stopped using the service of medical information systems, the records should be promptly deleted and the devices should be promptly discarded. When a record is deleted or a device is discarded, certificate of disposal should be submitted to medical institutions.	Information security oversight and management controls, including Storage Media Security controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google utilizes barcodes and asset tags to track the status and location of data center equipment from acquisition to installation, retirement, and destruction. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. Google hard drives leverage technologies, like Full Disk Encryption (FDE) and drive locking, to protect data at rest. Personable Identifiable Information (PII) on removable media leaving Google facilities is approved and encrypted.	-

			provision of it to medical institutions			When a hard drive is retired, authorized individuals verify that the disk is erased by writing zeros to the drive and performing a multiple-step verification process to help ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multistage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Google employs a static fully automated workflow tool to review, approve and track disks through the sanitization and destruction process.	
75	1. Human and organizational measures	1.8. Provision of records for data deletion	①Aquire of performance records for data deletion and provision of it to medical institutions	①-5	Agree with medical institutions on the purpose, scope, period, management of the records, safety grip actions and contact information when keeping records to the minimum extent in connection with support to medical institutions (including providing information to the administrative authorities) described in ①-4.	Not applicable. This is the customer's responsibility to respond to. Customer data will be always processed based on the contracted method. Google's Privacy Protection Responsibility: https://cloud.google.com/security/privacy/	-
76	1. Human and organizational measures	1.9. Management of subcontractors	①Dsiclosure of information to medical institution when subcontracting, and monitoring of subcontractor	①-1	When subcontracting information systems, explain to the manager of the medical institution in advance and obtain an agreement. In addition, clarify the management system of the information systems in the related subcontract.	Google is certified to the ISO27001 Standard, which regulates "Supplier Relationships" (ISO 27001:2013, Annex A.15). Information security oversight and management controls, including vendor security practices are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's Data Processing and Security Terms describe the process for Customers to object to subprocessor changes (DPST 11.4 Opportunity to Object to Subprocessor Changes). a. When any New Third Party Subprocessor is engaged during the Term, Google will, at least 30 days before the New Third Party Subprocessor starts processing any Customer Data, notify Customer of the engagement (including the name and location of the relevant subprocessor and the activities it will perform). b. Customer may, within 90 days after being notified of the engagement of a New Third Party Subprocessor, object by terminating the Agreement immediately by notifying Google. This termination right is Customer's sole and exclusive remedy if Customer objects to any New Third Party Subprocessor.	· ISO 27001 2013, Annex A.15

77	1. Human and organizational measures	1.9. Management of subcontractors	①Dsiclosure of information to medical institution when subcontracting, and monitoring of subcontractor	①-2	The subcontractor is required to comply with the same personal data guidelines as its own.	Google is certified to the ISO27001 Standard, which regulates "Supplier Relationships" (ISO 27001:2013, Annex A.15). Information security oversight and management controls, including vendor security practices are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google directly conducts virtually all data processing activities to provide our services. However, Google may engage some third-party suppliers to provide services related to Cloud Platform, including customer and technical support. Prior to onboarding third-party suppliers, Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms.	· ISO 27001 2013, Annex A.15
78	1. Human and organizational measures	1.9. Management of subcontractors	①Dsiclosure of information to medical institution when subcontracting, and monitoring of subcontractor	①-3	Include confidentiality obligations related to the consignment business in the contract related to the re-consignment.	Google is certified to the ISO27001 Standard, which regulates "Supplier Relationships" (ISO 27001:2013, Annex A.15). Information security oversight and management controls, including vendor security practices are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google directly conducts virtually all data processing activities to provide our services. However, Google may engage some third-party suppliers to provide services related to Cloud Platform, including customer and technical support. Prior to onboarding third-party suppliers, Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms.	· ISO 27001 2013, Annex A.15
79	1. Human and organizational measures	1.9. Management of subcontractors	①Dsiclosure of information to medical institution when subcontracting, and monitoring of subcontractor	①-4	Confirm with the subcontractor that the subcontractor personnel has the same confidentiality obligation as that of the company.	Google is certified to the ISO27001 Standard, which regulates "Supplier Relationships" (ISO 27001:2013, Annex A.15). Information security oversight and management controls, including vendor security practices are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google directly conducts virtually all data processing activities to provide our services. However, Google may engage some third-party suppliers to provide services related to Cloud Platform, including customer and technical support. Prior to onboarding third-party suppliers, Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms.	· ISO 27001 2013, Annex A.15
80	1. Human and organizational	1.9. Management of	①Dsiclosure of informatio	①-5	Agree with the medical institutions on the extent of report to medical institutions, content and conditions related to the provision of the information, when there	Please see Google's Terms of Service, which outline contractual obligations and agreements. Google Cloud Terms of Service: https://cloud.google.com/terms/ Google Workspace Terms of Services: https://workspace.google.com/terms/dpa_terms.html	-

	nal measures	subcontractors	n to medical institution when subcontracting, and monitoring of subcontractor		is a change on the medical information system, such as change in operational structure.	Section “1.4 Modification (a) To the services” mentions that “Google may make commercially reasonable updates to the Services from time to time. Google will inform Customer if Google makes a material change to the Services that has a material impact on Customer's use of the Services provided that Customer has subscribed with Google to be informed about such change.”.	
81	1. Human and organizational measures	1.9. Management of subcontractors	①Dsiclosure of information to medical institution when subcontracting, and monitoring of subcontractor	①-6	When part or all of the maintenance of medical information systems is entrusted to external operators, the external operators are requested to respond to the operational grip regulations and safety grip actions that are being implemented by the providers.	Google is certified to the ISO27001 Standard, which regulates "Supplier Relationships" (ISO 27001:2013, Annex A.15). Information security oversight and management controls, including vendor security practices are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google directly conducts virtually all data processing activities to provide our services. However, Google may engage some third-party suppliers to provide services related to Cloud Platform, including customer and technical support. Prior to onboarding third-party suppliers, Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms.	· ISO 27001 2013, Annex A.15
82	1. Human and organizational measures	1.9. Management of subcontractors	①Dsiclosure of information to medical institution when subcontracting, and monitoring of subcontractor	①-7	Regarding the implementation status of ①-6, request and confirm the report from external operators on a contract-by-contract basis or on a regular basis.	Google is certified to the ISO27001 Standard, which regulates "Supplier Relationships" (ISO 27001:2013, Annex A.15). Information security oversight and management controls, including vendor security practices are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google directly conducts virtually all data processing activities to provide our services. However, Google may engage some third-party suppliers to provide services related to Cloud Platform, including customer and technical support. Prior to onboarding third-party suppliers, Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms.	· ISO 27001 2013, Annex A.15
83	1. Human and organizational measures	1.9. Management of subcontractors	①Dsiclosure of information to medical institution	①-8	Ensure that the safety management measures and service levels of services provided by subcontractors are adequate.	Google is certified to the ISO27001 Standard, which regulates "Supplier Relationships" (ISO 27001:2013, Annex A.15). Information security oversight and management controls, including vendor security practices are reviewed and verified by a third party auditor for Google's SOC 2, Type II report.	· ISO 27001 2013, Annex A.15

			when subcontracting, and monitoring of subcontractor			Google directly conducts virtually all data processing activities to provide our services. However, Google may engage some third-party suppliers to provide services related to Cloud Platform, including customer and technical support. Prior to onboarding third-party suppliers, Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms.	
84	1. Human and organizational measures	1.9. Management of subcontractors	①Dsiclosure of information to medical institution when subcontracting, and monitoring of subcontractor	①-9	Periodically verify the implementation, operation, and maintenance of services carried out by subcontractors.	Google is certified to the ISO27001 Standard, which regulates "Supplier Relationships" (ISO 27001:2013, Annex A.15). Information security oversight and management controls, including vendor security practices are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google directly conducts virtually all data processing activities to provide our services. However, Google may engage some third-party suppliers to provide services related to Cloud Platform, including customer and technical support. Prior to onboarding third-party suppliers, Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms.	· ISO 27001 2013, Annex A.15
85	1. Human and organizational measures	1.9. Management of subcontractors	①Dsiclosure of information to medical institution when subcontracting, and monitoring of subcontractor	①-10	Periodical reports on implementation, operation and maintenance of services carried out by subcontractors should be provided beforehand and afterwards, and the report should be checked and confirmed by the provider.	Information security oversight and management controls, including vendor risk management practices are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google reviews the performance and security posture of sub-processors that support its products and services on a periodic basis.	-
86	1. Human and organizational measures	1.9. Management of subcontractors	①Dsiclosure of information to medical institution when subcontracting, and	①-11	Personnel to carry out the medical information system, such as staff of subcontractor must request access in advance and do not accept unauthorized personnel when carrying out the service.	Google is certified to the ISO27001 Standard, which regulates "Supplier Relationships" (ISO 27001:2013, Annex A.15). Information security oversight and management controls, including vendor security practices are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google has implemented an Sub-Data Processor Agreement (SDPA) to contracts with sub-processors who may have access to customer data. The SDPA defines the security and privacy obligations which the sub-processor must meet to satisfy Google 's obligations regarding customer data, prior to Google	· ISO 27001 2013, Annex A.15

			monitoring of subcontractor			granting such access. These obligations include requirements related to Personnel Security such as background checks.	
87	1. Human and organizational measures	1.9. Management of subcontractors	①Dsiclosure of information to medical institution when subcontracting, and monitoring of subcontractor	①-12	If a subcontractor enters the management area while services are in progress, carry an identification card with a facial photograph on the face of the ticket.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0	· ISO 27001 2013, Annex A.11
88	1. Human and organizational measures	1.9. Management of subcontractors	①Dsiclosure of information to medical institution when subcontracting, and monitoring of subcontractor	①-13	Procedures for entering the processing facility for implementation of the medical information system carried out by subcontractor, shall be the same as the procedures for entering and leaving for the staff of the information processing operator.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training.	· ISO 27001 2013, Annex A.11

						Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0	
89	1. Human and organizational measures	1.9. Management of subcontractors	①Dsiclosure of information to medical institution when subcontracting, and monitoring of subcontractor	①-14	When the medical information systems being changed by subcontractor, perform appropriate verification that security is still maintained.	Information security oversight and management controls, including vendor risk management practices are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google reviews the performance and security posture of sub-processors that support its products and services on a periodic basis.	-
90	1. Human and organizational measures	1.9. Management of subcontractors	①Dsiclosure of information to medical institution when subcontracting, and monitoring of subcontractor	①-15	When outsourcing the maintenance and inspection of medical information systems to external operators, implement the management measures in Section 6.8 C of "Guidelines for Safety management of Medical Information Systems, Version 5 (Health, Labor and Welfare Department, March 2017)".	Not applicable. This is the customer’s responsibility to respond to.	-
91	1. Human and organizatio	1.9. Management of	①Dsiclosure of informatio	①-16	When external operators perform medical information systems, it is desirable to perform operations under the	Google is certified to the ISO27001 Standard, which regulates "Supplier Relationships" (ISO 27001:2013, Annex A.15).	· ISO 27001 2013, Annex A.15

	nal measures	subcontractors	n to medical institution when subcontracting, and monitoring of subcontractor		management of authorized personnel of contractors or permanent staff of external operators.	Information security oversight and management controls, including vendor security practices are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google has implemented an Sub-Data Processor Agreement (SDPA) to contracts with sub-processors who may have access to customer data. The SDPA defines the security and privacy obligations which the sub-processor must meet to satisfy Google 's obligations regarding customer data, prior to Google granting such access. These obligations include requirements related to Personnel Security, including having written confidentiality agreements and performing background checks.	
92	1. Human and organizational measures	1.10. Measures for emergency preparation	①Performance of analysis on business impact related to provision of medical information system	①-1	Identify business processes related to medical information processing (including workers for carrying out processes), information processing facilities, etc.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	· ISO 27001 2013, Annex A.17.2, 12.3
93	1. Human and organizational measures	1.10. Measures for emergency preparation	①Performance of analysis on business impact related to provision of medical	①-2	Evaluate interrelationships between business processes.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural	· ISO 27001 2013, Annex A.17.2, 12.3

			information system			disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	
94	1. Human and organizational measures	1.10. Measures for emergency preparation	①Performance of analysis on business impact related to provision of medical information system	①-3	Clarify the priorities of business processes to continue business.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	· ISO 27001 2013, Annex A.17.2, 12.3
95	1. Human and organizational measures	1.10. Measures for emergency preparation	①Performance of analysis on business impact related to	①-4	Identify the impact of hardware and software failures on medical information systems on business processes.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services	· ISO 27001 2013, Annex A.17.2, 12.3

			provision of medical information system			themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	
96	1. Human and organizational measures	1.10. Measures for emergency preparation	①Performance of analysis on business impact related to provision of medical information system	①-5	Identify the effects and interactions of hardware and software faults occurring in medical information systems on other hardware and software, and identify the hardware and software with the greatest impact.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	· ISO 27001 2013, Annex A.17.2, 12.3
97	1. Human and organizatio	1.10. Measures for emergen	②Provision of business continuity	②-1	Establish a business continuity plan for medical information processing based on the priorities of business processes and medical information systems in the service provision of medical information systems.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report.	· ISO 27001 2013, Annex A.17.2, 12.3

	nal measures	cy preparation	plan regarding provision of medical information system and inspection of it by testing			Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	
98	1. Human and organizational measures	1.10. Measures for emergency preparation	②Provision of business continuity plan regarding provision of medical information system and inspection of it by testing	②-2	Review the planned business continuity plan in an appropriate manner, including simulated testing.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	· ISO 27001 2013, Annex A.17.2, 12.3

99	1. Human and organizational measures	1.10. Measures for emergency preparation	②Provision of business continuity plan regarding provision of medical information system and inspection of it by testing	②-3	Periodically review the business continuity plan.	Google is certified to the ISO27001 Standard, which regulates ""Redundancies"" (ISO27001:2013, Annex A.17.2) and ""Backup"" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	· ISO 27001 2013, Annex A.17.2, 12.3
100	1. Human and organizational measures	1.10. Measures for emergency preparation	②Provision of business continuity plan regarding provision of medical information system and inspection of it by testing	②-4	The planned business continuity plan should include the following items. ・ Prepare Plan ・ "emergency" judgment procedure ・ Calling related persons and setting up response headquarters ・ Degrade actions for equipment and workers and arrangements for alternative facilities ・ Actions to switch to alternative facilities, such as backup facilities ・ Considerations during the operation of the alternative facilities (e.g., procedures for operating the emergency accounts and considerations for synchronizing medical information to normal system after recovery) ・ Procedures and standards for determining the extent to which the problem has been expanded ・ Procedures and Standards for Determining Normal Recovery	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions.	· ISO 27001 2013, Annex A.17.12, 12.3

					・ Procedures for checking medical information systems after returning to normal (detection of unauthorized intrusion, information tampering, information corruption, etc.) ・ Contact system to administrative authorities, etc.	Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	
101	1. Human and organizational measures	1.10. Measures for emergency preparation	②Provision of business continuity plan regarding provision of medical information system and inspection of it by testing	②-5	Agree with the medical institutions on the content of services based on the formulated business continuity plans.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	· ISO 27001 2013, Annex A.17.2, 12.3
102	1. Human and organizational measures	1.10. Measures for emergency preparation	③Ensuring consistency after the restoration of medical information system	③-1	To ensure that the results of data processing performed in an emergency do not conflict after service restoration, measures should be taken to ensure the consistency of the data (e.g., stipulation of rules and verification methods).	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption.	· ISO 27001 2013, Annex A.17.2, 12.3

						Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	
103	1. Human and organizational measures	1.10. Measures for emergency preparation	④Provision of management manual for emergency user accounts and functions	④-1	Agree with the medical institutions on the measures to enable emergency user accounts and emergency functions.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2), and "Backup" (ISO27001:2013 Annex A 12.3.), and "Documented Operating Procedures" (ISO27001:2013, Annex A 12.1.1). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	· ISO 27001 2013, Annex A.17.2,12.3,12.1.1
104	1. Human and organizational measures	1.10. Measures for emergency preparation	④Provision of management manual for emergency user accounts and functions	④-2	Periodic reviews will be made on the status of use of user accounts in emergency situations.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2), and "Backup" (ISO27001:2013 Annex A 12.3.), and "Documented Operating Procedures" (ISO27001:2013, Annex A 12.1.1). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is	· ISO 27001 2013, Annex A.17.2,12.3,12.1.1

						automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	
105	1. Human and organizational measures	1.10. Measures for emergency preparation	④Provision of management manual for emergency user accounts and functions	④-3	When the user accounts used in the emergency is used, measures should be taken to enable the systems grip operator and the operator to confirm this promptly.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2), and "Backup" (ISO27001:2013 Annex A 12.3.), and "Documented Operating Procedures" (ISO27001:2013, Annex A 12.1.1). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	· ISO 27001 2013, Annex A.17.2,12.3,12.1.1
106	1. Human and organizational measures	1.10. Measures for emergency preparation	④Provision of management manual for emergency user	④-4	For the user accounts and emergency functions that were effective in the event of an emergency, the function should be disabled immediately after returning to normal status.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2), and "Backup" (ISO27001:2013 Annex A 12.3.), and "Documented Operating Procedures" (ISO27001:2013, Annex A 12.1.1). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a	· ISO 27001 2013, Annex A.17.2,12.3,12.1.1

			accounts and functions			solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	
107	1. Human and organizational measures	1.11. Measures for incidents caused by cyber attacks	①Immediate report to the medical institutions when the incident occured because of cyber attack	①-1	When the provision of services is hindered by cyber attacks, etc., the status of failures occurring in the service and the prospects for recovery should be promptly reported to medical institutions, etc.	Google is certified to the ISO27001 Standard, which regulates "Access to Networks and Network Services" (ISO27001:2013, Annex A.9.1.2), ""Network Controls"" (ISO27001:2013, Annex A.13.1.1). We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately.	· ISO 27001 2013, Annex A.9.1.2, 13.1.1
108	1. Human and organizational measures	1.11. Measures for incidents caused by cyber attacks	①Immediate report to the medical institutions when the incident occured	①-2	Agree with the medical institutions on the scope and conditions of data to be provided and reported to the administrative authorities, when the provision of service is hindered by cyber attacks and others.	Google is certified to the ISO27001 Standard, which regulates "Access to Networks and Network Services" (ISO27001:2013, Annex A.9.1.2), ""Network Controls"" (ISO27001:2013, Annex A.13.1.1). We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is	· ISO 27001 2013, Annex A.9.1.2, 13.1.1

			because of cyber attack			performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately.	
109	1. Human and organizational measures	1.11. Measures for incidents caused by cyber attacks	①Immediate report to the medical institutions when the incident occured because of cyber attack	①-3	Applications, platforms, server storages, etc. used to provide services should be installed in locations covered by the domestic law enforcement so that the documentations provided by medical institutions to government agencies based on laws can be smoothly submitted to the agencies.	Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27001:2013, Annex A.5) and Organization of Information Security (ISO27001:2013, Annex A.6). Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google allows cloud customers to determine data processing and storage location. The list of Google Cloud Platform products available by location is on our public website https://cloud.google.com/about/locations. Google Workspace Customer can choose where certain covered data should be stored at rest—either in the US, across Europe, or distributed globally. The Data Export tool provides export functionality for Google Workspace Core Services and Google Workspace Customer can store the data exported in your locations. The Data Export tool generally exports the same data that's available with Google Takeout for users, plus data that's available to admins only. What's included if you export data using the Data Export tool is on our public website. https://support.google.com/a/answer/100458?hl=en	· ISO 27001 2013, Annex A.5,6
110	1. Human and organizational measures	1.11. Measures for incidents caused by cyber attacks	②Maintenance of records such as logs for investigation of cause of cyber attacks	②-1	Take actions to preserve logs and other records required for investigating the causes of problems in the provision of services due to cyber hit, etc.	Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27001:2013, Annex A.5) and Organization of Information Security (ISO27001:2013, Annex A.6) and "Logging and Monitoring" (ISO 27001:2013, Annex A.12.4). Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google has defined policy and procedures to retain logs according to regulatory and Google retention requirements. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	· ISO 27001 2013, Annex A.5, 6, 12.4
111	1. Human and organizatio	1.12. Agreement on	①Agreements on extent of	①-1	Agree with the medical institutions on the extent of the contractor's role in protecting against tampering such	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001:2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report.	· ISO 27001 2013, Annex A.12.2

	nal measures	extent of responsibility and roles on network	Responsibility and roles when exchanging medical information externally		as the mixing of viruses and unauthorized messages in the network path.	Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/.	
112	1. Human and organizational measures	1.12. Agreement on extent of responsibility and roles on network	①Agreements on extent of Responsibility and roles when exchanging medical information externally	①-2	Agree with the medical institutions on the extent of the contractor's role in protecting against tampering such as the mixing of viruses and unauthorized messages in the network path.	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001:2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/.	· ISO 27001 2013, Annex A.12.2
113	1. Human and organizational measures	1.12. Agreement on extent of responsibility and roles on network	①Agreements on extent of Responsibility and roles when exchanging medical information externally	①-3	Agree with the medical institutions on the role of service providers, such as setting the routers in the building of medical institutions for the network, to prevent transmission and reception between VPNs connecting facilities through the routers.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Access to information resources, including data and the systems which store or process data, is authorized based on the principle of least privilege. Access to network devices is authenticated via user ID, password, security key, and/or certificate. External system users are identified and authenticated via the Google Accounts authentication system before access is granted.	· ISO 27001 2013, Annex A.9
114	1. Human and organizational measures	1.12. Agreement on extent of responsib	①Agreements on extent of Responsibility and	①-4	Agree with the medical institutions on the scope of responsibility and roles of contractor for management and quality of the network	Google is certified to the ISO27001 Standard, which regulates "Communications Security" (ISO 27001:2013, Annex A.13), and "Securing Application Service on Public Networks" ISO 27001:2013, (Annex A.14.1.2).	· ISO 27001 2013, Annex A.13,14.1.2

		ility and roles on network	roles when exchanging medical information externally			Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including management of external connections.	
115	1. Human and organizational measures	1.12. Agreement on extent of responsibility and roles on network	①Agreements on extent of Responsibility and roles when exchanging medical information externally	①-5	Clarify the communication procedures from the start point to the end point between medical institutions in normal operation and emergency, as well as responsibility of the network routes defined in Section 6.11 C of the MHLW Guidelines, 5th Edition 6.11. Agree with the medical institutions on the scope of responsibility and roles of a contractor clarified above..	Google Cloud and Google Workspace are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://workspace.google.com/terms/dpa_terms.html SLA: https://workspace.google.com/terms/sla.html https://cloud.google.com/terms/sla/	-
116	1. Human and organizational measures	1.12. Agreement on extent of responsibility and roles on network	①Agreements on extent of Responsibility and roles when exchanging medical information externally	①-6	Agree with the medical institutions on the security level of the information to be exchanged, so that the security level will not be lowered at the receiving side.	Google Cloud and Google Workspace are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://workspace.google.com/terms/dpa_terms.html SLA: https://workspace.google.com/terms/sla.html https://cloud.google.com/terms/sla/	-
117	1. Human and organizational measures	1.12. Agreement on extent of responsibility and roles on network	①Agreements on extent of Responsibility and roles when exchanging medical informatio	①-7	Agree with the medical institutions on the subcontractor's scope of responsibility and roles in medical institution's managers' accountability and management responsibility to the patient.	Google Cloud and Google Workspace are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://workspace.google.com/terms/dpa_terms.html SLA: https://workspace.google.com/terms/sla.html https://cloud.google.com/terms/sla/	-

			n externally				
118	1. Human and organizational measures	1.12. Agreement on extent of responsibility and roles on network	①Agreements on extent of Responsibility and roles when exchanging medical information externally	①-8	Agree with medical institutions on the terms and conditions of the security measures taken by the contractor, when managed medical information is to be viewed by the patient.	Google Cloud and Google Workspace are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://workspace.google.com/terms/dpa_terms.html SLA: https://workspace.google.com/terms/sla.html https://cloud.google.com/terms/sla/	-
119	1. Human and organizational measures	1.12. Agreement on extent of responsibility and roles on network	①Agreements on extent of Responsibility and roles when exchanging medical information externally	①-9	Agree with the medical institutions on the confidentiality level of the information to be exchanged (not lowering the confidentiality level at the recipient).	Google is certified to the ISO27001 Standard, which regulates "Cryptography" (ISO 27001:2013, Annex A.10) Encryption is used to protect user authentication and administrator sessions transmitted over the Internet. Remote access to Google corporate machines requires a Google issued digital certificate installed on the connecting device and two-factor authentication. Google publishes details about encryption and key management options for its Google Cloud Platform and Google Workspace products. To read more about key management and encryption, please see: https://cloud.google.com/security/encryption-at-rest/ https://cloud.google.com/security/encryption-in-transit/ https://services.google.com/fh/files/misc/google-workspace-encryption-wp.pdf Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including development of appropriate encryption measures.	· ISO 27001 2013, Annex A.10
120	1. Human and organizational measures	1.12. Agreement on extent of responsibility and roles on network	①Agreements on extent of Responsibility and roles when exchanging medical information externally	①-10	Agree with the medical institutions on the subcontractor's scope of responsibility and roles in medical institution's managers' accountability and management responsibility to the patient.	Google Cloud and Google Workspace are certified to the ISO27017 standard for cloud providers. Controls relating to confidentiality commitments are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://workspace.google.com/terms/dpa_terms.html SLA: https://workspace.google.com/terms/sla.html https://cloud.google.com/terms/sla/	-

Guidelines for Safety Management of Medical Information by Providers of Information Systems and Services Handling Medical Information

Handbook for Google Cloud and Google Workspace

121	1. Human and organizational measures	1.13. Quality Management of device and software	①Documenting the network diagram and specification related to medical information system	①-1	Prepare a configuration diagram of equipment and software in medical information systems.	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001:2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google Cloud and Google Workspace products are described in the "A. Overview of Operations" section of our SOC 2 Type II report which is reviewed and verified by a third party auditor. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	· ISO 27001 2013, Annex A.8.1, 8.3.2, 11.2.7, 12.5
122	1. Human and organizational measures	1.13. Quality Management of device and software	①Agreements on extent of Responsibility and roles when exchanging medical information externally	①-2	Create a network configuration diagram of the medical information system.	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001:2013, Annex A.8.1), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7), and "Documented Operating Procedures" (Annex A.12.1.1), and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google has documented procedures and checklists for configuring and installing new servers, routers and switches on the network. The network is documented in network diagrams and configuration documents describing the nature of, and requirements applicable to, Google's production networks. This documentation resides within an access-restricted portion of the corporate intranet. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	· ISO 27001 2013, Annex A.8.1,11.2.7,12.1.1, 12.5
123	1. Human and organizational measures	1.13. Quality Management of device and software	①Agreements on extent of Responsibility and roles when exchanging medical information externally	①-3	Prepare documents with descriptions of system requirements for the devices included in the configuration diagrams created in ①-1 and ①-2.	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001:2013, Annex A.8.1), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7), and "Documented Operating Procedures" (Annex A.12.1.1), and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google has documented procedures and checklists for configuring and installing new servers, routers and switches on the network. The network is documented in network diagrams and configuration documents describing the nature of, and requirements applicable to, Google's production networks. This documentation resides within an access-restricted portion of the corporate intranet. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	· ISO 27001 2013, Annex A.8.1,11.2.7,12.1.1, 12.5
124	1. Human and organizational measures	1.13. Quality Management of device and software	①Agreements on extent of Responsibility and roles when exchangin	①-4	Prepare a documentation related to the update measures of device and software which constitutes the medical information system, and the history of updates of them.	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001:2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google Cloud and Google Workspace products are described in the "A. Overview of Operations" section of our SOC 2 Type II report which is reviewed and verified by a third party auditor.	· ISO 27001 2013, Annex A.8.1,8.3.2,11.2.7,12.5

			g medical information externally			Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	
125	1. Human and organizational measures	1.13. Quality Management of device and software	①Agreements on extent of Responsibility and roles when exchanging medical information externally	①-5	In order to submit the data prepared in steps ①-1 to ①-4 in response to a request from a medical institutions, agree with them on the content, scope and conditions of the disclosure.	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001:2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google Cloud and Google Workspace products are described in the "A. Overview of Operations" section of our SOC 2 Type II report which is reviewed and verified by a third party auditor. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	· ISO 27001 2013, Annex A.8.1,8.3.2,11.2.7,12.5
126	1. Human and organizational measures	1.13. Quality Management of device and software	②Performance of beforehand inspection of installation or change of device and software	②-1	Evaluate the effects of changes in the information processing apparatus and software involved in maintenance.	Google is certified to the ISO27001 Standard, which regulates "Equipment Maintenance" (ISO 27001:2013, Annex A.11.2.4), "Change Management" (ISO27001:2013 Annex A 12.1.2) and "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14). Please see the Google Infrastructure Security Design Overview - https://cloud.google.com/security/security-design/ for more details. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including change management and system development procedures.	· ISO 27001 2013, Annex A.11.2.4, 12.1.2, 14
127	1. Human and organizational measures	1.13. Quality Management of device and software	②Performance of beforehand inspection of installation or change of device and software	②-2	Consider measures to minimize impact to ensure safe data storage when changes can adversely affect existing operations and equipments.	Google is certified to the ISO27001 Standard, which regulates "Change Management" (ISO27001:2013 Annex A 12.1.2) and "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14). Please see the Google Infrastructure Security Design Overview - https://cloud.google.com/security/security-design/ for more details. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including change management and system development procedures.	· ISO 27001 2013, Annex A.12.1.2,14

128	1. Human and organizational measures	1.13. Quality Management of device and software	②Performance of beforehand inspection of installation or change of device and software	②-3	Applications developed by information service providers themselves should be used for information processing. When an application development by an external developer is used, the application should be used after the safety has been fully verified in advance.	"Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14). Please see the Google Infrastructure Security Design Overview - https://cloud.google.com/security/security-design/ for more details. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including system development procedures.	· ISO 27001 2013, Annex A.14
129	1. Human and organizational measures	1.13. Quality Management of device and software	②Performance of beforehand inspection of installation or change of device and software	②-4	It is desirable to perform the verification process at both the binary code level and the source code level so that malicious code does not enter into the software.	Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14). Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including managing their system development process.	· ISO 27001 2013, Annex A.14
130	1. Human and organizational measures	1.13. Quality Management of device and software	②Performance of beforehand inspection of installation or change of device and software	②-5	Ensure that the software and operating system software for business use are fully tested before installation.	Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14). Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including managing their system development process.	· ISO 27001 2013, Annex A.14
131	1. Human and organizational measures	1.13. Quality Management of device	③Separation of operation environment and developin	③-1	When developing software, use development environments to avoid the effects on other operating software.	Google is certified to the ISO27001 Standard, which regulates "Separation of Development, Testing, and Operational Environments" (ISO 27001:2013, Annex A.12.1.4), " and Security in Development and Support Processes" (ISO 27001:2013, Annex A.14.2). Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	· ISO 27001 2013, Annex A.12.1.4,14.2

		and software	g environment				
132	1. Human and organizational measures	1.13. Quality Management of device and software	③Separation of operation environment and developing environment	③-2	In order to prevent malicious code from being mixed at the development facility, the development facility shall take measures against malicious programs when the development facility has connections to networks (such as the Internet) used by unspecified numbers.	Google is certified to the ISO27001 Standard, which regulates "Separation of Development, Testing, and Operational Environments" (ISO 27001:2013, Annex A.12.1.4), " and Security in Development and Support Processes" (ISO 27001:2013, Annex A.14.2). Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	· ISO 27001 2013, Annex A.12.1.4,14.2
133	1. Human and organizational measures	1.13. Quality Management of device and software	③Separation of operation environment and developing environment	③-3	Do not copy medical information stored in operation sites to development and testing facilities.	Google is certified to the ISO27001 Standard, which regulates "Separation of Development, Testing, and Operational Environments" (ISO 27001:2013, Annex A.12.1.4), " and Security in Development and Support Processes" (ISO 27001:2013, Annex A.14.2). Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	· ISO 27001 2013, Annex A.12.1.4,14.2
134	1. Human and organizational measures	1.13. Quality Management of device and software	③Separation of operation environment and developing environment	③-4	Do not place development code or development tools such as compilers on the operation system to avoid confusion of the operation system.	Google is certified to the ISO27001 Standard, which regulates "Separation of Development, Testing, and Operational Environments" (ISO 27001:2013, Annex A.12.1.4), " and Security in Development and Support Processes" (ISO 27001:2013, Annex A.14.2). Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	· ISO 27001 2013, Annex A.12.1.4,14.2
135	1. Human and organizational measures	1.13. Quality Management of device and software	③Separation of operation environment and developing environment	③-5	Do not place files or the like unnecessary for information processing on the operation system.	Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO 27001:2013, Annex A.14). Information security oversight and management controls, including software development controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support program file management activities.	· ISO 27001 2013, Annex A.14
136	1. Human and organizatio	1.14. Minimization of the	①Support of device and	①-1	Periodically confirm that the readability of equipments, media, etc. that store medical information is ensured.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and	· ISO 27001 2013, Annex A.17.1

	nal measures	change impact to the medical institution	software used in medical informatio n system			integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	
137	1. Human and organizatio nal measures	1.14. Minimizat ion of the change impact to the medical institution	①Support of device and software used in medical informatio n system	①-2	In cases where it may become difficult to ensure the readability of equipments and media that store medical information to be commissioned (deterioration of media, support of readers, etc.), take alternative measures promptly to ensure readability.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions.	· ISO 27001 2013, Annex A.17.1

						Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	
138	1. Human and organizational measures	1.14. Minimization of the change impact to the medical institution	①Support of device and software used in medical information system	①-3	Maintain and inspect each equipment according to the intervals and specifications specified by the manufacturer or supplier, and replace the equipment if necessary.	Google is certified to the ISO27001 Standard, which regulates "Equipment Maintenance" (ISO 27001:2013, Annex A.11.2.4), "Responsibility for Assets" (ISO 27001:2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), and "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	· ISO 27001 2013, Annex A.11.2.4, 8.1, 8.3.2, 11.2.7
139	1. Human and organizational measures	1.14. Minimization of the change impact to the medical institution	①Support of device and software used in medical information system	①-4	Carry out the inspection concerning the deterioration state periodically, and take necessary measures for the equipment related to the information system.	Google is certified to the ISO27001 Standard, which regulates "Equipment Maintenance" (ISO 27001:2013, Annex A.11.2.4), "Change Management" (ISO27001:2013 Annex A 12.1.2) and "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14). Google performs both preventative and regular maintenance on infrastructure hardware that supports production machines and network devices. System changes that may affect security, availability, processing integrity, or confidentiality are communicated to management and users who will be affected.	· ISO 27001 2013, Annex A.11.2.4,12.1.2,14
140	1. Human and organizational measures	1.14. Minimization of the change impact to the medical institution	①Support of device and software used in medical information system	①-5	For information systems, when support by providers of equipment, software, etc. is terminated, analyze the extent of impact on the services and take necessary measures.	Google has published the Terms of Service which outlines contractual obligations and agreements. Google Cloud Platform - Terms of Service: https://cloud.google.com/terms/ Section 1.4 (d) Discontinuation of Services mentions: "Google will notify Customer at least 12 months before discontinuing any Service (or associated material functionality) unless Google replaces such discontinued Service or functionality with a materially similar Service or functionality. Further, Google will notify Customer at least 12 months before significantly modifying a Customer-facing Google API in a backwards-incompatible manner. Nothing in this Section 1.4(d) (Discontinuation of Services) limits Google's ability to make changes required to comply with applicable law, address a material security risk, or avoid a substantial economic or material technical burden. This Section 1.4(d) (Discontinuation of Services) does not apply to pre-general availability Services, offerings, or functionality."	-

						Google Workspace - Terms of Service: https://workspace.google.com/terms/premier_terms.html Section 1.4 (e) Discontinuation of Core Services mentions :"Google will notify Customer at least 12 months before discontinuing any Core Service (or associated material functionality) unless Google replaces such discontinued Core Service or functionality with a materially similar Core Service or functionality. Nothing in this Section 1.4(e) (Discontinuation of Core Services) limits Google's ability to make changes required to comply with applicable law, address a material security risk, or avoid a substantial economic or material technical burden. This Section 1.4(e) (Discontinuation of Core Services) does not apply to Other Services or to pre-general availability Services, offerings, or functionality."	
141	1. Human and organizational measures	1.14. Minimization of the change impact to the medical institution	①Support of device and software used in medical information system	①-6	In cases where it becomes difficult to provide some or all of the services of medical information system due to deterioration of equipment, termination of support of equipment or software at providers or where there is a change in the services, the provider shall notify the medical institutions with a sufficient period for them to respond and take measures to minimize the impact on the medical institutions.	Google has published the Terms of Service which outlines contractual obligations and agreements. Google Cloud Platform - Terms of Service: https://cloud.google.com/terms/ Section 1.4 (d) Discontinuation of Services mentions: "Google will notify Customer at least 12 months before discontinuing any Service (or associated material functionality) unless Google replaces such discontinued Service or functionality with a materially similar Service or functionality. Further, Google will notify Customer at least 12 months before significantly modifying a Customer-facing Google API in a backwards-incompatible manner. Nothing in this Section 1.4(d) (Discontinuation of Services) limits Google's ability to make changes required to comply with applicable law, address a material security risk, or avoid a substantial economic or material technical burden. This Section 1.4(d) (Discontinuation of Services) does not apply to pre-general availability Services, offerings, or functionality." Google Workspace - Terms of Service: https://workspace.google.com/terms/premier_terms.html Section 1.4 (e) Discontinuation of Core Services mentions :"Google will notify Customer at least 12 months before discontinuing any Core Service (or associated material functionality) unless Google replaces such discontinued Core Service or functionality with a materially similar Core Service or functionality. Nothing in this Section 1.4(e) (Discontinuation of Core Services) limits Google's ability to make changes required to comply with applicable law, address a material security risk, or avoid a substantial economic or material technical burden. This Section 1.4(e) (Discontinuation of Core Services) does not apply to Other Services or to pre-general availability Services, offerings, or functionality."	-
142	1. Human and organizational measures	1.14. Minimization of the change impact to the medical institution	①Support of device and software used in medical information system	①-7	Agree with the medical institutions on the details and conditions of the response to medical institutions when some or all of the services are stopped or changed under the circumstances described in ①-6.	Google has published the Terms of Service which outlines contractual obligations and agreements. Google Cloud Platform - Terms of Service: https://cloud.google.com/terms/ Section 1.4 (d) Discontinuation of Services mentions: "Google will notify Customer at least 12 months before discontinuing any Service (or associated material functionality) unless Google replaces such discontinued Service or functionality with a materially similar Service or functionality. Further, Google will notify Customer at least 12 months before significantly modifying a Customer-facing Google API in a backwards-incompatible manner. Nothing in this Section 1.4(d) (Discontinuation of Services) limits Google's ability to make changes required to comply with applicable law, address a material security risk, or avoid a substantial economic or material technical burden. This Section 1.4(d) (Discontinuation of Services) does not apply to pre-general availability Services, offerings, or functionality."	-

						Google Workspace - Terms of Service: https://workspace.google.com/terms/premier_terms.html Section 1.4 (e) Discontinuation of Core Services mentions :"Google will notify Customer at least 12 months before discontinuing any Core Service (or associated material functionality) unless Google replaces such discontinued Core Service or functionality with a materially similar Core Service or functionality. Nothing in this Section 1.4(e) (Discontinuation of Core Services) limits Google's ability to make changes required to comply with applicable law, address a material security risk, or avoid a substantial economic or material technical burden. This Section 1.4(e) (Discontinuation of Core Services) does not apply to Other Services or to pre-general availability Services, offerings, or functionality."	
143	1. Human and organizational measures	1.14. Minimization of the change impact to the medical institution	②Minimization of suspended time of medical information system caused by maintenance	②-1	Plan and implement maintenance work of the information processing apparatus and software so as to minimize the stop time of the information processing work.	Google is certified to the ISO27001 Standard, which regulates "Equipment Maintenance" (ISO 27001:2013, Annex A.11.2.4). Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	· ISO 27001 2013, Annex A.11.2.4
144	1. Human and organizational measures	1.14. Minimization of the change impact to the medical institution	②Minimization of suspended time of medical information system caused by maintenance	②-2	Include the extent impact by the maintenance work and assumed time requirement for the restitution when the maintenance work is not completed to the advance notice of maintenance operation.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions.	· ISO 27001 2013, Annex A.17.2
145	1. Human and organizational	1.14. Minimization of the	②Minimization of suspende	②-3	When carrying out the maintenance work, take appropriate measures to prevent medical institutions	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report.	· ISO 27001 2013, Annex A.17.2

	nal measures	change impact to the medical institution	d time of medical informatio n system caused by maintena nce		from becoming unavailable, and include the procedures in the operation grip regulations.	Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions.	
146	1. Human and organizatio nal measures	1.14. Minimizat ion of the change impact to the medical institution	②Minimiz ation of suspende d time of medical informatio n system caused by maintena nce	②-4	Agree with the medical institutions on the procedures specified in ②-3 and indicate it to them. Agree with the medical institutions about items required for maintenance based on this procedure.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions.	· ISO 27001 2013, Annex A.17.2
147	1. Human and organizatio nal measures	1.14. Minimizat ion of the change impact to the medical institution	②Minimiz ation of suspende d time of medical informatio n system caused by	②-5	Agree with the medical institutions on the procedures mentioned in ②-3, if there is a matter that medical institution should handle with.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data	· ISO 27001 2013, Annex A.17.2

			maintenance			centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions.	
148	1. Human and organizational measures	1.14. Minimization of the change impact to the medical institution	③Response to the suspension and specification change of medical information system	③-1	When a part or all of the service is stopped or the service is changed (minor version upgrades are not included), take measures to minimize the impact on the medical institutions using the service, and notify them with a sufficient period for the medical institutions to respond.	Google has published the Terms of Service which outlines contractual obligations and agreements. Google Cloud Platform - Terms of Service: https://cloud.google.com/terms/ Section 1.4 (d) Discontinuation of Services mentions: "Google will notify Customer at least 12 months before discontinuing any Service (or associated material functionality) unless Google replaces such discontinued Service or functionality with a materially similar Service or functionality. Further, Google will notify Customer at least 12 months before significantly modifying a Customer-facing Google API in a backwards-incompatible manner. Nothing in this Section 1.4(d) (Discontinuation of Services) limits Google's ability to make changes required to comply with applicable law, address a material security risk, or avoid a substantial economic or material technical burden. This Section 1.4(d) (Discontinuation of Services) does not apply to pre-general availability Services, offerings, or functionality." Google Workspace - Terms of Service: https://workspace.google.com/terms/premier_terms.html Section 1.4 (e) Discontinuation of Core Services mentions :"Google will notify Customer at least 12 months before discontinuing any Core Service (or associated material functionality) unless Google replaces such discontinued Core Service or functionality with a materially similar Core Service or functionality. Nothing in this Section 1.4(e) (Discontinuation of Core Services) limits Google's ability to make changes required to comply with applicable law, address a material security risk, or avoid a substantial economic or material technical burden. This Section 1.4(e) (Discontinuation of Core Services) does not apply to Other Services or to pre-general availability Services, offerings, or functionality."	-
149	1. Human and organizational measures	1.14. Minimization of the change impact to the medical institution	③Response to the suspension and specification change of medical information system	③-2	Return the entrusted medical information to medical institutions in case of ③-1. Agree on the range of data to be returned (data type, period, etc.), data format (data item, item details, file format), return method, and conditions with the medical institutions. When the contents of the agreement are changed after the start of service use by medical institutions or other institutions, countermeasures are taken in accordance with ③-1.	Google has published the Terms of Service which outlines contractual obligations and agreements. Google Cloud Platform - Terms of Service: https://cloud.google.com/terms/ Section 1.4 (d) Discontinuation of Services mentions: "Google will notify Customer at least 12 months before discontinuing any Service (or associated material functionality) unless Google replaces such discontinued Service or functionality with a materially similar Service or functionality. Further, Google will notify Customer at least 12 months before significantly modifying a Customer-facing Google API in a backwards-incompatible manner. Nothing in this Section 1.4(d) (Discontinuation of Services) limits Google's ability to make changes required to comply with applicable law, address a material security risk, or avoid a substantial economic or material technical burden. This Section 1.4(d) (Discontinuation of Services) does not apply to pre-general availability Services, offerings, or functionality."	-

						Google Workspace - Terms of Service: https://workspace.google.com/terms/premier_terms.html Section 1.4 (e) Discontinuation of Core Services mentions :"Google will notify Customer at least 12 months before discontinuing any Core Service (or associated material functionality) unless Google replaces such discontinued Core Service or functionality with a materially similar Core Service or functionality. Nothing in this Section 1.4(e) (Discontinuation of Core Services) limits Google's ability to make changes required to comply with applicable law, address a material security risk, or avoid a substantial economic or material technical burden. This Section 1.4(e) (Discontinuation of Core Services) does not apply to Other Services or to pre-general availability Services, offerings, or functionality."	
150	1. Human and organizational measures	1.14. Minimization of the change impact to the medical institution	③Response to the suspension and specification change of medical information system	③-3	Regarding the return of data in ③-2, it shall be carried out in accordance with Version 5 "Interoperability and standardize of information" of the MHLW Guidelines, and the contents thereof shall be agreed with the medical institutions. Incidentally, since the data to be returned may include data obtained by lossy compression (image data, etc.) or conversion (password, etc.) performed by the contractor, also agree on this with the medical institutions.	Google provides functionalities which may change the customers' original data format and customers are responsible for understanding the specifications provided by Google, such as: https://cloud.google.com/terms/data-processing-terms https://workspace.google.com/terms/dpa_terms.html https://support.google.com/a/answer/100458 https://support.google.com/accounts/answer/3024190. https://cloud.google.com/bigquery/docs/exporting-data https://cloud.google.com/sql/docs/mysql/import-export/exporting https://cloud.google.com/spanner/docs/import-export-csv https://cloud.google.com/datastore/docs/export-import-entities	-
151	1. Human and organizational measures	1.14. Minimization of the change impact to the medical institution	③Response to the suspension and specification change of medical information system	③-4	Agree with the medical institutions on the measures (except for the response to ③-2 in the transition support and others) and conditions to be taken to them when some or all part of the services including change to the services (minor version upgrades are not included) are stopped in ③-1.	Google has published the Terms of Service which outlines contractual obligations and agreements. Google Cloud Platform - Terms of Service: https://cloud.google.com/terms/ Section 1.4 (d) Discontinuation of Services mentions: "Google will notify Customer at least 12 months before discontinuing any Service (or associated material functionality) unless Google replaces such discontinued Service or functionality with a materially similar Service or functionality. Further, Google will notify Customer at least 12 months before significantly modifying a Customer-facing Google API in a backwards-incompatible manner. Nothing in this Section 1.4(d) (Discontinuation of Services) limits Google's ability to make changes required to comply with applicable law, address a material security risk, or avoid a substantial economic or material technical burden. This Section 1.4(d) (Discontinuation of Services) does not apply to pre-general availability Services, offerings, or functionality." Google Workspace - Terms of Service: https://workspace.google.com/terms/premier_terms.html Section 1.4 (e) Discontinuation of Core Services mentions :"Google will notify Customer at least 12 months before discontinuing any Core Service (or associated material functionality) unless Google replaces such discontinued Core Service or functionality with a materially similar Core Service or functionality. Nothing in this Section 1.4(e) (Discontinuation of Core Services) limits Google's ability to make changes required to comply with applicable law, address a material security risk, or avoid a substantial economic or material technical burden. This Section 1.4(e) (Discontinuation of Core Services) does not apply to Other Services or to pre-general availability Services, offerings, or functionality."	-

152	1. Human and organizational measures	1.14. Minimization of the change impact to the medical institution	③Response to the suspension and specification change of medical information system	③-5	When the use of services of medical institutions is terminated due to medical institutions or other reasons, the countermeasures shown in ③-2 and ③-3 should be taken.	Please see Google's Terms of Service, which outline contractual obligations and agreements. Google Cloud Terms of Service: https://cloud.google.com/terms/data-processing-terms; Data Processing and Security Terms (Customers) :https://cloud.google.com/terms/data-processing-terms Google Workspace Terms of Service: https://workspace.google.com/terms/dpa_terms.html; Data Processing Amendment to Google Workspace and/or Complementary Product Agreement: https://workspace.google.com/terms/dpa_terms.html Section 9.1 Access; Rectification; Restricted Processing; Portability mentions: "During the Term, Google will enable Customer, in a manner consistent with the functionality of the Services, to access, rectify and restrict processing of Customer Data, including via the deletion functionality provided by Google as described in Section 6.1 (Deletion by Customer), and to export Customer Data."	-
153	1. Human and organizational measures	1.14. Minimization of the change impact to the medical institution	③Response to the suspension and specification change of medical information system	③-6	The procedures for items ③-1 to ③-5 shall be included in the Operation grip Rules, etc.	Google has published the Terms of Service which outlines contractual obligations and agreements. Google Cloud Platform - Terms of Service: https://cloud.google.com/terms/; Data Processing and Security Terms (Customers): https://cloud.google.com/terms/data-processing-terms Google Workspace - Terms of Service: https://workspace.google.com/terms/premier_terms.html; Data Processing Amendment: https://workspace.google.com/terms/dpa_terms.html	-
154	2.Physical Measures	2.1. Entry/exit management	①Autorization and entry/exit management to the installation location of device and elements	①-1	Grip to enter and leave security boundaries, such as where equipments and media are installed, should be controlled by individual identification systems to identify people who enter and leave the service. When it is difficult to do so, measures are taken to identify the person entering or leaving, for example, changing the personal identification number or the like necessary for entering or leaving on a weekly basis.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google’s focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged.	· ISO 27001 2013, Annex A.11

						To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0	
155	2.Physical Measures	2.1. Entry/exit management	①Authorization and entry/exit management to the installation location of device and elements	①-2	Restrict access to the installation location of the equipments and media, so that only authorised personnel can enter and leave.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0	· ISO 27001 2013, Annex A.11
156	2.Physical Measures	2.1. Entry/exit management	①Authorization and entry/exit management to the installation location of device and elements	①-3	In order to restrict access to rooms where medical information is stored by installing medical information systems, a person must be authenticated by installing one or both of a manned reception and a mechanical authentication device to ensure the authenticity of entering and leaving theaters.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored, logged and periodically approved for appropriateness. Google adheres to all building and facility requirements in the region where its data centers are located.	· ISO 27001 2013, Annex A.11

157	2.Physical Measures	2.1. Entry/exit management	①Authorization and entry/exit management to the installation location of device and elements	①-4	When management entrances and exits using mechanical authentication devices without having to accept personnel, use authentication devices using a plurality of factors including one or more biometrics.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0	· ISO 27001 2013, Annex A.11
158	2.Physical Measures	2.1. Entry/exit management	①Authorization and entry/exit management to the installation location of device and elements	①-5	Acquire certification histories for both personnel acceptance and mechanical access management, periodically verify the histories to ensure that there is no suspicious activity.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged.	· ISO 27001 2013, Annex A.11

						To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0	
159	2.Physical Measures	2.1. Entry/exit management	①Autorization and entry/exit management to the installation location of device and elements	①-6	Specify the time that the staff of contractors can stay in the office according to their duties.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored, logged and periodically approved for appropriateness. Employees with access must follow documented policies and procedures for the type of secured areas they are working in.	· ISO 27001 2013, Annex A.11
160	2.Physical Measures	2.1. Entry/exit management	①Autorization and entry/exit management to the installation location of device and elements	①-7	As authentication elements used in mechanical authentication devices, it is desirable to combine authentication devices such as hardware tokens or IC cards, storage elements such as personal identification numbers (PIN) or passwords and biometrics.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers	· ISO 27001 2013, Annex A.11

						Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0	
161	2.Physical Measures	2.1. Entry/exit management	①Autorization and entry/exit management to the installation location of device and elements	①-8	Management of access (including the review of access records) to the installation location of the devices and equipment shall be performed periodically.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0	· ISO 27001 2013, Annex A.11
162	2.Physical Measures	2.2. Locking management, key management	①Locking and key management of server rack and cabinet	①-1	When installing a medical information system, etc. in the area occupied by the contractor, take the following physical safety control measures. Confirm that the same measures are taken when using the data center and server environment (proprietary server, virtual private server, etc.) operated by an external company. ・In order to prevent unauthorized accesses to server equipment and others in which medical information is stored, locking management and key management of server racks shall be performed.	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A.11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos:	· ISO 27001 2013, Annex A.11

						Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0	
163	2.Physical Measures	2.2. Locking management, key management	①Autorization and entry/exit management to the installation location of device and elements	①-2	Locking management shall be performed for security boundaries such as installation locations of devices, equipments and others.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0	· ISO 27001 2013, Annex A.11
164	2.Physical Measures	2.2. Locking management, key management	①Autorization and entry/exit management to the installation location of device and elements	①-3	Locking management shall be performed for racks and others which stores server.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved	· ISO 27001 2013, Annex A.11

						employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0	
165	2.Physical Measures	2.2. Locking management, key management	①Autorization and entry/exit management to the installation location of device and elements	①-4	Locking management shall be performed for cabinets and others which store media and others.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0	· ISO 27001 2013, Annex A.11
166	2.Physical Measures	2.2. Locking management, key management	①Autorization and entry/exit management to the installation location of device	①-5	Cabinets for storing electronic media should be provided with a physically secure locking device with adequate security, and the key management should be carefully considered.	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001:2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor	· ISO 27001 2013, Annex A.8.1,8.3.2,11.2.7,12.5

			and elements			without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	
167	2.Physical Measures	2.2. Locking management, key management	①Authorization and entry/exit management to the installation location of device and elements	①-6	External operators operating data centres shall confirm that the security is guaranteed against physical unauthorised manipulation by person outside the management of contractors, by implementing safety measures equivalent to contractor's facilities.	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A.11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0	· ISO 27001 2013, Annex A.11.2
168	2.Physical Measures	2.2. Locking management, key management	①Authorization and entry/exit management to the installation location of device and elements	①-7	Lock the server rack where the medical information system is installed, and perform reliable key management so that only personnel of the defined contractors can handle the key.	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A.11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos:	· ISO 27001 2013, Annex A.11.2

						Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0	
169	2.Physical Measures	2.2. Locking management, key management	①Authorization and entry/exit management to the installation location of device and elements	①-8	Record the worker, work start time, work end time, work contents and others of the work performed by the contractors when they unlock the server rack in which the medical information system is installed.	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A.11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0	· ISO 27001 2013, Annex A.11.2
170	2.Physical Measures	2.2. Locking management, key management	①Authorization and entry/exit management to the installation location of device and elements	①-9	When an external provider who operates the data center unlocks the server rack and performs work, contact in advance as a rule, and confirm that medical information systems and medical information are not affected.	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A.11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0	· ISO 27001 2013, Annex A.11.2
171	2.Physical Measures	2.2. Locking	①Authorization and	①-10	In order to prevent other operators who enter the same data center from knowing that the medical information	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A.11.2).	· ISO 27001 2013, Annex A.11.2

		management, key management	entry/exit management to the installation location of device and elements		system is a medical information system, information that can identify the type of information handled, the function of the system, etc. should not be made visible from the outside.	Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0	
172	2.Physical Measures	2.2. Locking management, key management	①Authorization and entry/exit management to the installation location of device and elements	①-11	As for the locking device of the server rack in which the medical information system is installed, it is desirable to combine an authentication device such as a hardware token or an IC card, a storage element such as a personal identification number (PIN), a password, biometrics information, and the like.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0	· ISO 27001 2013, Annex A.11
173	2.Physical Measures	2.2. Locking manage	①Authorization and entry/exit	①-12	Make sure that sufficient security is ensured against unauthorized access by persons outside the management of the contractor.	Google is certified to the ISO27001 Standard, which regulates "Supplier Relationships" (ISO 27001:2013, Annex A.15).	· ISO 27001 2013, Annex A.15

		ment, key manage ment	managem ent to the installatio n location of device and elements			Information security oversight and management controls, including vendor security practices are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google directly conducts virtually all data processing activities to provide our services. However, Google may engage some third-party suppliers to provide services related to Cloud Platform, including customer and technical support. Prior to onboarding third-party suppliers, Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms.	
174	2.Physical Measures	2.2. Locking manage ment, key manage ment	①Autoriz ation and entry/exit managem ent to the installatio n location of device and elements	①-13	Information that allows identification of the type of information and function of the system should not be seen from the outside of the storage location (including rack and storage) of the equipment and media.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google’s focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0	· ISO 27001 2013, Annex A.11
175	2.Physical Measures	2.2. Locking manage ment, key manage ment	①Autoriz ation and entry/exit managem ent to the installatio n location of device	①-14	Items ①-1 to ①-13 shall be stipulated in the Operation management standards.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google’s focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are	· ISO 27001 2013, Annex A.11

			and elements			monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0	
176	2.Physical Measures	2.3. Monitoring of unauthorised access	①Monitoring of intrusion to the facilities handling medical information by surveillance camera	①-1	When installing a medical information system, etc. in the area occupied by the contractor, take the following physical safety control measures. Confirm that the same measures are taken when using the data center and server environment (proprietary server, virtual private server, etc.) operated by an external company. ・In order to prevent unauthorized activities such as interception and theft, the wall, ceiling, and floor sections that divide the room must have a sufficient thickness to provide measures such as constant monitoring with a surveillance camera, storage of image records, and periodic detection of unauthorized devices. ・Introducing an intrusion detection device (such as surveillance cameras) to prevent unauthorized physical intrusion into buildings and rooms.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. Google’s focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Google adheres to all building and facility requirements in the region where its data centers are located.	・ISO 27001 2013, Annex A.11
177	2.Physical Measures	2.3. Monitoring of unauthorised access	①Monitoring of intrusion to the facilities handling	①-2	Monitoring images of security cameras and the like shall be recorded, grip shall be performed with a fixed period limit, and measures shall be taken to allow for post-referencing as needed.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google’s focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed	・ISO 27001 2013, Annex A.11

			medical information by surveillance camera			electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0	
178	2.Physical Measures	2.3. Monitoring of unauthorised access	①Monitoring of intrusion to the facilities handling medical information by surveillance camera	①-3	Install surveillance cameras or the like in places where equipments, media, and the like are physically stored, store the records, and check the status to confirm that there are no unauthorized entrances and exits.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google’s focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers	· ISO 27001 2013, Annex A.11

						Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0	
179	2.Physical Measures	2.3. Monitoring of unauthorised access	①Monitoring of intrusion to the facilities handling medical information by surveillance camera	①-4	A surveillance camera or the like is used to appropriately monitor the area where the service operation and maintenance terminal or the like is installed.	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A.11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0	· ISO 27001 2013, Annex A.11
180	2.Physical Measures	2.3. Monitoring of unauthorised access	②Obliging staff of subcontractors to wear staff certificate	②-1	During the job in the area occupied by the contractor, it is mandatory to carry the staff ID card of the information processing business operator in which the facial photograph of the staff is recorded on the visible side of the card, so that it can be identified when a person who is not the staff of the information processing business enters the area.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers	· ISO 27001 2013, Annex A.11

						Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0	
181	2.Physical Measures	2.3. Monitoring of unauthorised access	②Obliging staff of subcontractors to wear staff certificate	②-2	The staff member of the contractor must ask and confirm the identity, if they see a person who is not the staff member of the contractor in the exclusive area of the contractor.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0	· ISO 27001 2013, Annex A.11
182	2.Physical Measures	2.3. Monitoring of unauthorised access	②Obliging staff of subcontractors to wear staff certificate	②-3	Strict issue and revocation management of staff certificates should be performed. For example, ・immediately notify the manager when the loss or illegal use of the staff certificate is suspected. ・reliably collect and discard the staff certificates when the staff of contractors leaves the office.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved	· ISO 27001 2013, Annex A.11

						employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0	
183	2.Physical Measures	2.4. Measures in backup facility	①Performing physical safety measures to the backup facilities	①-1	If it is necessary for continuation of the medical information system provided to medical institutions, an alternative information processing facility for continuing the medical information systems, such as a backup facility for medical information to be entrusted, shall be established, and physical safety measures presented in this guideline shall be provided for those facilities.	Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google has created a highly redundant, geographically dispersed network of secure data centers around the world. Google selects data centers based on a site selection process that includes geographical separation between data centers as a major factor. This reduces the data centers' susceptibility to the same environmental or infrastructure threats or hazards, such as weather events, earthquakes or large-scale power outages. Google hardware, software and data centers around the world provide consistent, trusted security, ease maintenance and offer a transparent solution to customers. Google's processing sites are not labeled as primary or alternate. All processing sites may act as primary for some processes and alternate for others. Thus, there is no distinction between the safeguarding of the primary processing site from the alternate processing site. All processing sites meets the required basic security and access restrictions for a secured posture.	-
184	2.Physical Measures	2.5. Restriction on bringing private asset	①Restiriction on bringing private asset to medical information processing facilities	①-1	Do not allow personal properties that are not related to the performance of tasks within medical information processing facilities.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved	· ISO 27001 2013, Annex A.11

						employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0	
185	2.Physical Measures	2.5. Restriction on bringing private asset	①Restiriction on bringing private asset to medical information processing facilities	①-2	Restrict the bringing in of personal properties irrelevant to the performance of services to the installation locations of equipments and media.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0	· ISO 27001 2013, Annex A.11
186	2.Physical Measures	2.6. Measures for theft of device	①Attachement of anti-theft chain to the important devices	①-1	Attach anti-theft chains to significant equipments, such as PCs, where the personal data resides.	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A.11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are	· ISO 27001 2013, Annex A.8.1,8.3.2,11.2.7,12.5

						monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers	
187	2.Physical Measures	2.7. Measures for peeking	①Measures for peeking	①-1	Make a layout of equipment in the room so that no unauthorized access to the terminal screen on which medical information or the like is displayed will be viewed.	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A.11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers	· ISO 27001 2013, Annex A.11.2
188	2.Physical Measures	2.7. Measures for peeking	①Measures for peeking	①-2	In order to prevent peeping while the personal data is displayed, measures should be taken, such as pasting sheets of countermeasures against peeping on the operation terminal.	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A.11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos:	· ISO 27001 2013, Annex A.11.2

						Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers	
189	2.Physical Measures	2.8. Measures for disaster	①Measures for Earthquake, flood, thunderbolt, fire, and blackouts	①-1	The facilities for physically preserving the equipment and media shall be installed in buildings that have functions and structures that can withstand disasters (earthquakes, water damage, thunder, fires, etc. and associated power outages) and that take measures against disaster failures (crippling, etc.).	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.	· ISO 27001 2013, Annex A.11
190	2.Physical Measures	2.8. Measures for disaster	①Measures for Earthquake, flood, thunderbolt, fire, and blackouts	①-2	Agree with the medical institutions on the architectures in which the facilities are installed.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.	· ISO 27001 2013, Annex A.11
191	2.Physical Measures	2.8. Measures for disaster	①Measures for Earthquake, flood,	①-3	Be careful not to damage the fire equipment in the event of a fire.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report.	· ISO 27001 2013, Annex A.11

			thunderbolt, fire, and blackouts			Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers	
192	2.Physical Measures	2.8. Measures for disaster	①Measures for Earthquake, flood, thunderbolt, fire, and blackouts	①-4	To prohibit smoking and eating and drinking in the room where the medical information system is installed.	Google is certified to the ISO27001 Standard, which regulates "Information Security Awareness, Education and Training" (ISO 27001:2013, Annex A.7.2.2), Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All Google contractors undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new contractors agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.	· ISO 27001 2013, Annex A.7.2.2
193	2.Physical Measures	2.8. Measures for disaster	①Measures for Earthquake, flood, thunderbolt, fire, and blackouts	①-5	When placing a fuel-readable object and a liquid in the room where the medical information system is placed, care should be taken not to adversely affect the device, such as maintaining a sufficient distance between the device and providing a dedicated storage facility.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust detection of environmental elements, including heat, fire, smoke and water detection. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, smoke, and water detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.	· ISO 27001 2013, Annex A.11

Guidelines for Safety Management of Medical Information by Providers of Information Systems and Services Handling Medical Information

Handbook for Google Cloud and Google Workspace

194	2.Physical Measures	2.8. Measures for disaster	①Measures for Earthquake, flood, thunderbolt, fire, and blackouts	①-6	The following security management measures should be implemented for server racks where medical-information systems are installed. ・Ensure that you do not fall in the event of an earthquake. ・There must be sufficient air conditioning equipments to prevent failure by ii thermal, and the server rack must be fully ventilated. ・A physical locking device with adequate security strength should be provided on the door and the key management should be fully taken into consideration.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google's data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located and maintains facilities that comply with best practices to minimize damage due to natural disasters.	· ISO 27001 2013, Annex A.11
195	3.Technical measures	3.1. Introduction of user authentication	①Adoption of methods identifying user uniquely	①-1	When registering, editing, and deleting information in a medical information system, design and implementation should be performed so as to log on in order to identify the user and confirm the authority.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and Google Workspace products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	· ISO 27001 2013, Annex A.9
196	3.Technical measures	3.1. Introduction of user authentication	①Adoption of methods identifying user uniquely	①-2	Issue accounts so that users of information systems can be identified and identified. (The ID is not shared by a plurality of users, except for the ID (non interactive ID) used by the information systems to use other information systems.)	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report.	· ISO 27001 2013, Annex A.9

						For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and Google Workspace products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	
197	3.Technical measures	3.1. Introduction of user authentication	①Adoption of methods identifying user uniquely	①-3	Authentication is performed to prevent user spoofing and the like.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and Google Workspace products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	· ISO 27001 2013, Annex A.9
198	3.Technical measures	3.1. Introduction of user authentication	①Adoption of methods identifying user uniquely	①-4	Issue of IDs to persons who are engaged in the operation or development of medical information systems or issues of IDs to persons who have management authorities is required to be minimized, and periodical inventory of ID should be taken.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report.	· ISO 27001 2013, Annex A.9

						For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and Google Workspace products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	
199	3.Technical measures	3.1. Introduction of user authentication	②Preparation of temporary authentication method	②-1	Alternative means and procedures for temporarily authenticating when some physical medium, physical information or the like is required for user authentication even if there is no exceptionally such medium or the like shall be defined in advance.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	· ISO 27001 2013, Annex A.9
200	3.Technical measures	3.1. Introduction of user authentication	②Preparation of temporary authentication method	②-2	In the case where the alternative means and procedure are used, the difference in risk from the case of the original user authentication method is minimized.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	· ISO 27001 2013, Annex A.9
201	3.Technical measures	3.1. Introduction of	②Preparation of temporary	②-3	Records and management of records should be made to enable later tracing even when the medical	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9).	· ISO 27001 2013, Annex A.9

		user authentication	authentication method		information systems are used by alternative methods and procedures.	Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	
202	3.Technical measures	3.1. Introduction of user authentication	②Preparation of temporary authentication method	②-4	Agree with the medical institutions on the methods of authentication for temporary user in addition.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	· ISO 27001 2013, Annex A.9
203	3.Technical measures	3.1. Introduction of user authentication	③Measures when leaving desk for long time	③-1	Locking or logging off the terminal when leaving or not using the terminal to prevent the use of a third party in advance.	Google is certified to the ISO27001 Standard, which regulates "Unattended user equipment" (ISO 27001:2013, Annex A.11.2.8). The organization has security guidance that requires users to lock their computers and mobile devices when unattended.	· ISO 27001 2013, Annex A.11.2.8
204	3.Technical measures	3.1. Introduction of user authentication	③Measures when leaving desk for long time	③-2	The Operation grip Regulations and other regulations specify that measures are to be taken to prevent clearing screens, etc. on the operation and maintenance terminals, etc. of services.	Google is certified to the ISO27001 Standard, which regulates "Clear desk and clear screen policy" (ISO 27001:2013, Annex A.11.2.9). The organization has security guidance that requires users to lock their computers and mobile devices when unattended.	· ISO 27001 2013, Annex A.11.2.9
205	3.Technical measures	3.1. Introduction of user authentication	③Measures when leaving desk for long time	③-3	Agree with the medical institutions on the leakage prevention measures, such as a clear screen to the user devices which is installed in the medical institutions and is able to view medical institutions.	Google is certified to the ISO27001 Standard, which regulates "Clear desk and clear screen policy" (ISO 27001:2013, Annex A.11.2.9). The organization has security guidance that requires users to lock their computers and mobile devices when unattended.	· ISO 27001 2013, Annex A.11.2.9
206	3.Technical measures	3.1. Introduction of	③Measures when leaving	③-4	In order to reduce the risk of hijacking a terminal or a session, a session for which a certain interruption time	Google is certified to the ISO27001 Standard, which regulates "Unattended user equipment" (ISO 27001:2013, Annex A.11.2.8).	· ISO 27001 2013, Annex A.11.2.8

		user authentication	desk for long time		has elapsed after the user logs on can be blocked or forcibly logged off.	Google has enabled session locks on the end user computers in the form of a password protected screen-saver after 15 minutes of inactivity on the user's computer. The screen-saver remains locked until the user signs back into their computer. Google also enforces encrypted session for the connections to the production environment, thus preventing man in the middle attacks or hijacking of idle sessions.	
207	3.Technical measures	3.1. Introduction of user authentication	③Measures when leaving desk for long time	③-5	Agree with the medical institutions on the specific application of the actions in absence to user terminals.	Google is certified to the ISO27001 Standard, which regulates "Unattended user equipment" (ISO 27001:2013, Annex A.11.2.8). Google has enabled session locks on the end user computers in the form of a password protected screen-saver after 15 minutes of inactivity on the user's computer. The screen-saver remains locked until the user signs back into their computer. Google also enforces encrypted session for the connections to the production environment, thus preventing man in the middle attacks or hijacking of idle sessions.	· ISO 27001 2013, Annex A.11.2.8
208	3.Technical measures	3.1. Introduction of user authentication	④Definition of safe password	④-1	For passwords, set a quality standard including content that password should be hard to estimate by third parties, and make sure that all password meet this standard.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	· ISO 27001 2013, Annex A.9
209	3.Technical measures	3.1. Introduction of user authentication	④Definition of safe password	④-2	Agree with medical institutions etc. for the password policy.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	· ISO 27001 2013, Annex A.9
210	3.Technical measures	3.1. Introduction of user	④Definition of safe password	④-3	Set the expiration date for the password and force the operator to change the password periodically. However, when the user is a patient or persons equivalent to the patient, in addition to particularly	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report.	· ISO 27001 2013, Annex A.9

		authentication			promote them not to set the password used in other services, avoid requesting them to change the password periodically.	Google has followed NIST guidance (SP 800-63c) and has not enforced password history and rotation requirements. However Google has provided mechanisms for external customers to integrate their SSO via SAML. Given this, Google believes that our password policies provides "equivalent or better security" than the 2G3M standard requirements. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Strong authentication and access controls are implemented to restrict access to Google Cloud production systems, internal support tools, and customer data. Machine-level access restriction relies on Google-developed distributed authentication service based on Transport Layer Security (TLS) certificates which helps to positively identify the resource access requester. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	
211	3.Technical measures	3.1. Introduction of user authentication	④Definition of safe password	④-4	Perform generation management of the password and operate it so that previously set password cannot be set to the extent necessary for security maintenance.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	· ISO 27001 2013, Annex A.9
212	3.Technical measures	3.1. Introduction of user authentication	④Definition of safe password	④-5	When issuing a password, issue a password for logon to a provisional medical information system generated from a random number, and take measures against password theft risk by forcibly changing the password at the time of first logon.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	· ISO 27001 2013, Annex A.9

213	3.Technical measures	3.1. Introduction of user authentication	④Definition of safe password	④-6	Ensure workers do not use the automatic logon function to store passwords in the system.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	· ISO 27001 2013, Annex A.9
214	3.Technical measures	3.1. Introduction of user authentication	④Definition of safe password	④-7	When the user registers and changes the password for the medical information system, consider a mechanism for ensuring that the predetermined quality is satisfied, introduce a program for generating a password by a random number, or introduce a system which does not permit the user to set a password having a low quality.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Google personnel are required to authenticate using valid credentials prior to resetting their password. Passwords are managed and configured in accordance with a set of password construction, protection, and management guidelines, which enforce the following: • Minimum length • Complexity • History • Idle time lockout setting Password configuration requirements are enforced by internal systems. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google’s internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google’s security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee’s authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and Google Workspace products. Support services are only	· ISO 27001 2013, Annex A.9

						provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	
215	3.Technical measures	3.1. Introduction of user authentication	④Definition of safe password	④-8	Keep the information used for identification and authentication confidential so that only the individual knows those information.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Strong authentication and access controls are implemented to restrict access to Google Cloud production systems, internal support tools, and customer data. Machine-level access restriction relies on Google-developed distributed authentication service based on Transport Layer Security (TLS) certificates which helps to positively identify the resource access requester. This service also offers transport encryption to enhance data confidentiality in transit. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	· ISO 27001 2013, Annex A.9
216	3.Technical measures	3.1. Introduction of user authentication	④Definition of safe password	④-9	When an initial password is issued to a user, access to the information system is prohibited unless the password is changed at the time of initial use.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	· ISO 27001 2013, Annex A.9
217	3.Technical measures	3.1. Introduction of user authentication	④Definition of safe password	④-10	Passwords other than the initial password are set by the user himself or principal, and the user is requested to set the contents which can be known only by the user himself or herself.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	· ISO 27001 2013, Annex A.9

218	3.Technical measures	3.1. Introduction of user authentication	④Definition of safe password	④-11	When a password is set, a plurality of character types (alphanumeric characters, uppercase letters, lowercase letters, symbols, etc.) are used, and a rule is made up of character strings or the like having a sufficiently secure length, such as eight characters or more.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Google personnel are required to authenticate using valid credentials prior to resetting their password. Passwords are managed and configured in accordance with a set of password construction, protection, and management guidelines, which enforce the following: • Minimum length • Complexity • History • Idle time lockout setting Password configuration requirements are enforced by internal systems. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and Google Workspace products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	· ISO 27001 2013, Annex A.9
219	3.Technical measures	3.1. Introduction of user authentication	④Definition of safe password	④-12	When introducing products to be used for services, not only are initial passwords changed, but necessary accounts are inventoried, and unnecessary initial passwords are deleted.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report.	· ISO 27001 2013, Annex A.9

						Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	
220	3.Technical measures	3.1. Introduction of user authentication	④Definition of safe password	④-13	A mechanism shall be used in which the input of the password before the change is requested when the password is changed, and the password change is not accepted for a certain period of time when the input of the password before the change fails a certain number of times or more.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Users are required to authenticate using valid credentials prior to resetting their password. Passwords are managed in accordance with a set of password construction, protection and management guidelines, which enforce the following: a) Minimum length b) Complexity c) History d) Idle time lockout setting Password security requirements are stipulated in the security guidelines and controls (password complexity, expiration, etc.) are built into systems to help ensure that Google password standards are enforced.	· ISO 27001 2013, Annex A.9
221	3.Technical measures	3.1. Introduction of user authentication	④Definition of safe password	④-14	Set a certain refractory time for re-entry when password entry is unsuccessful. A mechanism that does not accept re-entry for a certain period of time should be adopted when logon fails continuously. If this happens, a mechanism should be introduced to send alert messages to the systems management.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Users are required to authenticate using valid credentials prior to resetting their password. Passwords are managed in accordance with a set of password construction, protection and management guidelines, which enforce the following: a) Minimum length b) Complexity c) History d) Idle time lockout setting Password security requirements are stipulated in the security guidelines and controls (password complexity, expiration, etc.) are built into systems to help ensure that Google password standards are enforced.	· ISO 27001 2013, Annex A.9
222	3.Technical measures	3.1. Introducti	⑤Adoption of multi-	⑤-1	As an authentication element used at the time of logon, it is desirable to implement multi-factor authentication	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9).	· ISO 27001 2013, Annex A.9

		on of user authentication	factor authentication		by combining an authentication device such as a hardware token or an IC card, a storage element such as a personal identification number (PIN), a password, biometrics information, and the like.	Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	
223	3.Technical measures	3.1. Introduction of user authentication	⑤Adoption of multi-factor authentication	⑤-2	Authentication related to the use of a medical information system by a person engaged in the operation or development of the information system, or authentication related to the use of person who have management should be multi factor authentication.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	· ISO 27001 2013, Annex A.9
224	3.Technical measures	3.1. Introduction of user authentication	⑤Adoption of multi-factor authentication	⑤-3	Agree with the medical institutions on the authentication method to be adopted for user authentication.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	· ISO 27001 2013, Annex A.9
225	3.Technical measures	3.1. Introduction of user authentication	⑤Adoption of multi-factor authentication	⑤-4	When an authentication method using a fixed ID and password is adopted for user authentication, an effort is made to provide a function that can cope with adoption of an authentication method that does not rely solely on a fixed ID and password. The MHLW Guidelines describe that two-factor authentication is assumed to be "C. Minimum Guidelines" in Chapter 6.5 of the MHLW Guidelines after about 10 years from the	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report.	· ISO 27001 2013, Annex A.9

					release of the 5th Edition of the MHLW Guidelines (May 2017).	Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	
226	3.Technical measures	3.2. Management of Access rights	①Access management to control access rights on minimum need base	①-1	For manipulation of medical information systems, access management corresponding to powers and duties of medical institutions should be enabled, and prevent creation, browsing, editing and deletion of information by those who do not have legitimate access authorities.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer’s data from that of other customers and users, even when it’s stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google’s internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google’s security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee’s authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and Google Workspace products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	· ISO 27001 2013, Annex A.9
227	3.Technical measures	3.2. Management of Access rights	①Access management to control access rights on minimum need base	①-2	Settings of access control according to the job category of the user of the medical institution, etc. shall be indicated to the medical institution, etc., and necessary consultations shall be made with the medical institution, etc. and agreements shall be agreed, including sharing of roles related to the work to be actually set up.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer’s data from that of other customers and users, even when it’s stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google’s internal employee	· ISO 27001 2013, Annex A.9

						portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and Google Workspace products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	
228	3.Technical measures	3.2. Management of Access rights	①Access management to control access rights on minimum need base	①-3	Organize security requirements regarding access control of each components of medical information system (information processing apparatus and software).	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	· ISO 27001 2013, Annex A.9
229	3.Technical measures	3.2. Management of Access rights	①Access management to control access rights on minimum need base	①-4	To appropriately group information and control access to groups of information so as to minimize workers having authority to access each information.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and Google Workspace products.	· ISO 27001 2013, Annex A.9

						Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	
230	3.Technical measures	3.2. Management of Access rights	①Access management to control access rights on minimum need base	①-5	Establish the minimum necessary access privileges in consideration of the content of work, and set the privileges in the application and the operation system.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and Google Workspace products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	· ISO 27001 2013, Annex A.9
231	3.Technical measures	3.2. Management of Access rights	①Access management to control access rights on minimum need base	①-6	It is desirable to periodically verify that the prescribed access control policy is appropriately reflected as an access control mechanism such as a file, directory permission, database access, and the like.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google periodically reviews logical access to all systems to ensure appropriateness of access. Further, Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	· ISO 27001 2013, Annex A.9

232	3.Technical measures	3.2. Management of Access rights	①Access management to control access rights on minimum need base	①-7	In order to prevent unauthorized access to medical information commissioned when performing scheduled maintenance and operations, measures such as setting authority should be taken.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google periodically reviews logical access to all systems to ensure appropriateness of access. Further, Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	· ISO 27001 2013, Annex A.9
233	3.Technical measures	3.2. Management of Access rights	①Access management to control access rights on minimum need base	①-8	Take actions (encryption of databases, etc.) to ensure that systems grip personnel, operation personnel, maintenance personnel, etc. do not perform unintended browsing.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google periodically reviews logical access to all systems to ensure appropriateness of access. Further, Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	· ISO 27001 2013, Annex A.9
234	3.Technical measures	3.2. Management of Access rights	②Restriction of access to medical information	②-1	Measures should be taken to classify medical information and other information.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer’s data from that of other customers and users, even when it’s stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google’s internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google’s security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee’s authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and Google Workspace products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams	· ISO 27001 2013, Annex A.9

						Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	
235	3.Technical measures	3.2. Management of Access rights	②Restriction of access to medical information	②-2	For medical information, access control should be performed according to the information category.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and Google Workspace products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	· ISO 27001 2013, Annex A.9
236	3.Technical measures	3.2. Management of Access rights	②Restriction of access to medical information	②-3	When providing services with resources using virtualization technologies, measures are taken to ensure that section grip can be performed logically.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies.	· ISO 27001 2013, Annex A.9

						Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and Google Workspace products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	
237	3.Technical measures	3.2. Management of Access rights	②Restriction of access to medical information	②-4	Based on the Service Specification Adaptation Disclosure Form, agree with medical institutions to set up categories of information assets by medical institutions and to respond to access control settings.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and Google Workspace products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	· ISO 27001 2013, Annex A.9
238	3.Technical measures	3.3. Management of ID and password	①Management and operation of user access and ID	①-1	The user should be identified by a unique user ID on the medical information systems.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report.	· ISO 27001 2013, Annex A.9

						For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and Google Workspace products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	
239	3.Technical measures	3.3. Management of ID and password	①Management and operation of user access and ID	①-2	Introduce a mechanism to eliminate duplicated existing IDs when issuing userIDs.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and Google Workspace products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	· ISO 27001 2013, Annex A.9
240	3.Technical measures	3.3. Management of	①Management and	①-3	Group ID which shares ID with number of workers shall not be used in principle, but if this is necessary for business reason, a mechanism to switch individual	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9).	· ISO 27001 2013, Annex A.9

		ID and password	operation of user access and ID		user ID to group ID after the login with individual user ID in order to identify who performed the manipulation.	Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google periodically reviews logical access to all systems to ensure appropriateness of access. Further, Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	
241	3.Technical measures	3.3. Management of ID and password	①Management and operation of user access and ID	①-4	Issuance of user IDs should be limited to the minimum number of people required for management of medical-information systems.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and Google Workspace products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	· ISO 27001 2013, Annex A.9
242	3.Technical measures	3.3. Management of ID and password	①Management and operation of user access and ID	①-5	The userID used in the past should not be reused in order to reliably specify the worker when the monitoring log is inspected.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google periodically reviews logical access to all systems to ensure appropriateness of access. Further, Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams.	· ISO 27001 2013, Annex A.9

						Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	
243	3.Technical measures	3.3. Management of ID and password	①Management and operation of user access and ID	①-6	It is desirable to periodically confirm that the accessible range of the worker ID permitted to access is as permitted (that is, that it has not been tampered with).	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google periodically reviews logical access to all systems to ensure appropriateness of access. Further, Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	· ISO 27001 2013, Annex A.9
244	3.Technical measures	3.3. Management of ID and password	①Management and operation of user access and ID	①-7	In order to detect the use or attempt of an unauthorized account by the user himself/herself, it is desirable to display the success date and time if the previous log on is successful, and to display the failure date and time together with a warning message indicating that an unauthorized log on attempt by a third party may have been made.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Users are required to authenticate using valid credentials prior to resetting their password. Passwords are managed in accordance with a set of password construction, protection and management guidelines, which enforce the following: a) Minimum length b) Complexity c) History d) Idle time lockout setting Password security requirements are stipulated in the security guidelines and controls (password complexity, expiration, etc.) are built into systems to help ensure that Google password standards are enforced.	· ISO 27001 2013, Annex A.9
245	3.Technical measures	3.3. Management of ID and password	①Management and operation of user access and ID	①-8	In order to prevent unauthorized account use, it is desirable to limit the days of the week and the time zone required for operation to the days of the week when users are allowed to log on.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google’s internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google’s security policies. Approvals are managed by workflow tools	· ISO 27001 2013, Annex A.9

						that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and Google Workspace products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	
246	3.Technical measures	3.3. Management of ID and password	①Management and operation of user access and ID	①-9	When an unauthorized user or a third party tries to log on, displaying "password is different" provides a clue to the existence of the user ID. Therefore, it is preferable to display only a message that does not give special information such as "Authentication failed" or simply redisplay the logon prompt.	Google is certified to the ISO27001 Standard, which regulates "User access management" (ISO 27001:2013, Annex A.9.2). Google native authentication requires a minimum 8 character complex password. Tenants can set the maximum or increase the minimum. A built-in Password Monitor is visible to the end user upon password creation and to the System Administrators of the tenant whom can decide to force a password change on any user that is later detected to have a password that is weak. Google's native authentication has protections in place that would detect a brute force attack and challenge the user to solve a Captcha and would auto lock the account if suspicious activity is detected. The tenant's System Administrators can reset that account for the end user.	· ISO 27001 2013, Annex A.9.2
247	3.Technical measures	3.3. Management of ID and password	①Management and operation of user access and ID	①-10	It is recommended that a reasonable approval process be developed when logging on is required outside the specified time for emergency work.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and Google Workspace products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	· ISO 27001 2013, Annex A.9
248	3.Technical measures	3.3. Manage	①Management	①-11	Change password or invalidate accounts immediately and notify administrator, when unauthorized access to	Google is certified to the ISO27001 Standard, which regulates "Access to Networks and Network Services" (ISO27001:2013, Annex A.9.1.2), "Network Controls" (ISO27001:2013, Annex A.13.1.1).	· ISO 27001 2013, Annex A.9.1.2,13.1

		ment of ID and password	and operation of user access and ID		medical information systems is suspected or the password may be known to third parties.	We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately.	
249	3.Technical measures	3.3. Management of ID and password	①Management and operation of user access and ID	①-12	When a user changes or retires, the user ID must be stopped immediately.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users) for access to the production environment. For Google employees account creation at Google begins in an automated process triggered by HR, whereby an onboarding system assigns a unique user ID to the new employee (including vendors, contractors, and temporary employees). This user ID is unique and will never be reused for another individual. If the employee leaves Google the user ID is not deleted, rather the accounts associated with it are disabled, and the user ID may only be reused if the same employee returns to Google.	・ISO 27001 2013, Annex A.9
250	3.Technical measures	3.3. Management of ID and password	①Management and operation of user access and ID	①-13	Check periodically that no unnecessary user IDs remain.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google periodically reviews logical access to all systems to ensure appropriateness of access. Further, Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	· ISO 27001 2013, Annex A.9

251	3.Technical measures	3.3. Management of ID and password	②Records of minimum use and performance content of privileged ID	②-1	Issuance of privilege IDs should be limited to the minimum required.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and Google Workspace products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	· ISO 27001 2013, Annex A.9
252	3.Technical measures	3.3. Management of ID and password	②Records of minimum use and performance content of privileged ID	②-2	Restrict user IDs that can be promoted to privileged users.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and Google Workspace products.	· ISO 27001 2013, Annex A.9

						Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	
253	3.Technical measures	3.3. Management of ID and password	②Records of minimum use and performance content of privileged ID	②-3	When using privileges, record the details of the operation.	Google is certified to the ISO27001 Standard, which regulates ""Access Control"" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google has implemented monitoring tools to detect and report application vulnerabilities. Google also maintains user access logs for privileged access and for access to user data. Logical access to audit logs is restricted to authorized personnel.	· ISO 27001 2013, Annex A.9
254	3.Technical measures	3.3. Management of ID and password	②Records of minimum use and performance content of privileged ID	②-4	Disable direct logon with privileged IDs from other than management terminals.	Google is certified to the ISO27001 Standard, which regulates ""Access Control"" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	· ISO 27001 2013, Annex A.12.1
255	3.Technical measures	3.3. Management of ID and password	②Records of minimum use and performance content of privileged ID	②-5	It is preferable to separate the accounts according to the type of privileges and restrict accesses to files and directories.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer’s data from that of other customers and users, even when it’s stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google’s internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google’s security policies.	· ISO 27001 2013, Annex A.9

						Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and Google Workspace products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	
256	3.Technical measures	3.3. Management of ID and password	②Records of minimum use and performance content of privileged ID	②-6	If possible as a function of the medical information system, it is desirable to limit the range of commands and utilities that can be used with the privilege ID to the minimum range necessary for business, and to prevent unauthorized activities such as tampering and deletion of important commands, utilities, and logs.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and Google Workspace products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	· ISO 27001 2013, Annex A.9
257	3.Technical measures	3.3. Management of ID and password	③Management of ID and password	③-1	Users should keep their password secret and keep them in a safe place to protect from access, modification, or disposal by others.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report.	· ISO 27001 2013, Annex A.9

						Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	
258	3.Technical measures	3.3. Management of ID and password	③Management of ID and password	③-2	Before using the medical information system or software, inventory default accounts, maintenance accounts established by the manufacturing subcontractor, and delete or change passwords for unnecessary accounts.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google periodically reviews logical access to all systems to ensure appropriateness of access. Further, Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	· ISO 27001 2013, Annex A.9
259	3.Technical measures	3.3. Management of ID and password	③Management of ID and password	③-3	Store information in a form that does not allow easy restoration of passwords, such as storing passwords with hash values, encryption, etc.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9) and "Cryptography" (ISO 27001:2013, Annex A.10). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Internal passwords are subject to cryptographic hashing to mitigate the risk of unauthorized disclosure or modification.	· ISO 27001 2013, Annex A.9, 10
260	3.Technical measures	3.3. Management of ID and password	③Management of ID and password	③-4	To preserve the authenticity and integrity of files storing password-related data, security measures should be adopted, such as obtaining and verifying hash values of files, giving and verifying digital signatures to files, and encrypting and storing files. Also, restrict access by ordinary users.	Google is certified to the ISO27001 Standards, which regulates "Operational Procedures and Responsibilities" (ISO 27001:2013, Annex A.12.1). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. System changes that may affect security, availability, processing integrity, or confidentiality are communicated to management and users who will be affected. Integrity checks are in place at the application level and file system level to help ensure data integrity. At the application level, checksum comparison is performed to protect against upload corruptions. File system consistency checks are also deployed at the storage layer using user-level programs which verify the integrity of the data.	· ISO 27001 2013, Annex A.12
261	3.Technical measures	3.3. Management of	③Management of	③-5	When information such as passwords is leaked(including attacks from an unauthorized third party), immediately invalidate the ID, and re-issue new	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9).	· ISO 27001 2013, Annex A.9

		ID and password	ID and password		log-in information based on the procedures prepared in advance. Then, notify to the users promptly.	Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	
262	3.Technical measures	3.3. Management of ID and password	③Management of ID and password	③-6	When there is a risk of leakage of information such as a password, a measure is taken so that the password can be invalidated and changed after notifying the user himself of the fact.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	· ISO 27001 2013, Annex A.9
263	3.Technical measures	3.4. Acquisition and inspection of logs	①Acquisition and inspection of log	①-1	Logs (user activity, events generated by the device, system failures, system use conditions, etc.) are recorded and stored for a certain period of time.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google has implemented monitoring tools to detect and report application vulnerabilities. Google also maintains user access logs for privileged access and for access to user data. Logical access to audit logs is restricted to authorized personnel. Audit logs are monitored continuously using a Google proprietary Security Information and Event Management system to detect intrusion attempts and other security related events. Google has procedures in place to dispose of confidential information according to Google data retention and deletion policy. Additionally, Google maintains policies regarding the return, transfer, and disposal of user data and makes these policies available to customers.	· ISO 27001 2013, Annex A.9
264	3.Technical measures	3.4. Acquisition and inspection of logs	①Acquisition and inspection of log	①-2	Regularly check logs to detect fraud and system abnormality.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report.	· ISO 27001 2013, Annex A.9

						Google maintains a Data Security Policy that governs access to data and mechanisms to prevent and detect unauthorized access.	
265	3.Technical measures	3.4. Acquisition and inspection of logs	①Acquisition and inspection of log	①-3	The following items are assumed to be recorded in the log. ・ User information (user ID, permission/prohibition of logon, time and time of use, details of execution work, access source IP address in case of network access) ・ File and data access, modification, and delete records (user ID, accessibility, use time and time, use content, target file or data type) ・ Database operation records (user ID, availability of connection and work, time and time of use, details of execution use, IP address of access source, details of setting change) ・ Apply of correction patches (user ID, changed file) ・ Privileged operations (privilege acquirer ID, availability of privilege acquisition, use time and time, execution use content) ・ System startup and shutdown events ・ Start and end events of the log acquisition function ・ Removing an External Device ・ Event logs of security devices such as IDSs and IPS ・ Logs generated by the operation of services and applications (including logs related to time synchronization)	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and Google Workspace products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	· ISO 27001 2013, Annex A.9
266	3.Technical measures	3.4. Acquisition and inspection of logs	①Acquisition and inspection of log	①-4	If possible, log data will be aggregated, analyzed and managed on a dedicated log server for the purpose of centralizing logs and reliably detecting problems in one place.	Google is certified to the ISO27001 Standard, which regulates "Event Logging" (ISO 27001:2013, Annex A.12.4.1). Security monitoring controls are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Audit logs are monitored continuously using a Google proprietary Security Information and Event Management system to detect intrusion attempts and other security related events. Security alerts are generated for further investigation based on predefined thresholds. These monitoring tools issue automated alerts to security personnel.	· ISO 27001 2013, Annex A.12.4.1
267	3.Technical measures	3.4. Acquisition and inspection of logs	①Acquisition and inspection of log	①-5	Acquire logs necessary for auditing for updating library programs related to the operation system.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report.	· ISO 27001 2013, Annex A.9

						Google has implemented monitoring tools to detect and report application vulnerabilities. Google also maintains user access logs for privileged access and for access to user data. Logical access to audit logs is restricted to authorized personnel.	
268	3.Technical measures	3.4. Acquisition and inspection of logs	①Acquisition and inspection of log	①-6	Acquire logs for duplicate and use of system operation information (system and service configuration files, etc.) as audit trails.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and Google Workspace products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	· ISO 27001 2013, Annex A.9
269	3.Technical measures	3.4. Acquisition and inspection of logs	①Acquisition and inspection of log	①-7	Ensure that access records by persons engaged in the operation/development of the medical information system or persons with administrative authority are reviewed regularly and that there is no unauthorized access.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google has implemented monitoring tools to detect and report application vulnerabilities. Google also maintains user access logs for privileged access and for access to user data. Logical access to audit logs is restricted to authorized personnel.	· ISO 27001 2013, Annex A.9
270	3.Technical measures	3.4. Acquisition and inspection of logs	①Acquisition and inspection of log	①-8	Agree with medical institutions on the provision of information on ①-7.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google has implemented monitoring tools to detect and report application vulnerabilities. Google also maintains user access logs for privileged access and for access to user data. Logical access to audit logs is restricted to authorized personnel.	· ISO 27001 2013, Annex A.9

271	3.Technical measures	3.4. Acquisition and inspection of logs	①Acquisition and inspection of log	①-9	Agree with the medical institution, in case of not having functions to acquire logs.	Google is certified to the ISO27001 Standard, which regulates "Event Logging" (ISO 27001:2013, Annex A.12.4.1). Security monitoring controls are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Audit logs are monitored continuously using a Google proprietary Security Information and Event Management system to detect intrusion attempts and other security related events. Security alerts are generated for further investigation based on predefined thresholds. These monitoring tools issue automated alerts to security personnel.	· ISO 27001 2013, Annex A.12.4.1
272	3.Technical measures	3.4. Acquisition and inspection of logs	①Acquisition and inspection of log	①-10	Those who are engaged in the maintenance of the medical information system or who have administrative authority, shall access the medical information system for the purpose of his/her duties by account issued by each agent.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and Google Workspace products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	· ISO 27001 2013, Annex A.9
273	3.Technical measures	3.4. Acquisition and inspection of logs	①Acquisition and inspection of log	①-11	Work done in the account specified in ①-10, is recorded and saved by the log in a form that can specify the personal information accessed.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google has implemented monitoring tools to detect and report application vulnerabilities. Google also maintains user access logs for privileged access and for access to user data. Logical access to audit logs is restricted to authorized personnel.	· ISO 27001 2013, Annex A.9

274	3.Technical measures	3.4. Acquisition and inspection of logs	①Acquisition and inspection of log	①-12	An operation result performed in maintenance of the medical information system is recorded and managed by an operation log.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google has implemented monitoring tools to detect and report application vulnerabilities. Google also maintains user access logs for privileged access and for access to user data. Logical access to audit logs is restricted to authorized personnel.	· ISO 27001 2013, Annex A.9
275	3.Technical measures	3.4. Acquisition and inspection of logs	①Acquisition and inspection of log	①-13	The status of the accessed medical information is reviewed using the obtained operation log or the like.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google has implemented monitoring tools to detect and report application vulnerabilities. Google also maintains user access logs for privileged access and for access to user data. Logical access to audit logs is restricted to authorized personnel.	· ISO 27001 2013, Annex A.9
276	3.Technical measures	3.4. Acquisition and inspection of logs	①Acquisition and inspection of log	①-14	In order to verify the log, it is desirable to develop a system capable of quickly confirming the user's ID and information identifier (asset register entry number), generation time series, access time series, and various indicators, and narrowing down the information type and access time.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and Google Workspace products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	· ISO 27001 2013, Annex A.9
277	3.Technical measures	3.4. Acquisition and	②Access restriction and	②-1	Apply the following management measures to properly protect logs from unauthorized accesses. ・ Restrict user and operation to access log data.	Google is certified to the ISO27001 Standard, which regulates ""Access Control"" (ISO 27001:2013, Annex A.9).	· ISO 27001 2013, Annex A.9

		inspection of logs	external storage to prevent tampering and deletion of logs		・ In order to avoid a situation where the log cannot be acquired due to excess capacity, the storage capacity of the log server should always be monitored, and measures for writing to an electronic medium and capacity enhancement are taken. ・ Detection and prevention measures are taken against unauthorized alteration and deletion of log data.	Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google maintains a Data Security Policy that governs access to data and mechanisms to prevent and detect unauthorized access.	
278	3.Technical measures	3.4. Acquisition and inspection of logs	③Syncronizing the clock to standard time	③-1	In order to accurately verify the cause of accident, etc. by using the log, the time of all the server devices, etc. of the medical information system should be synchronized with the standard time provided by the time server, etc.	Google is certified to the ISO27001 Standard, which regulates "Clock synchronization" (ISO 27001:2013, Annex A.14.4.4). Google uses a syncronized time-service protocol to ensure all systems have a common time reference. Google makes their NTP protocol public as well for use by customers. https://developers.google.com/time/	· ISO 27001 2013, Annex A.14.4.4
279	3.Technical measures	3.4. Acquisition and inspection of logs	③Syncronizing the clock to standard time	③-2	It is desirable to periodically verify that the times of all the server devices and the like of the medical information system are synchronized with the standard time provided by the time server and the like.	Google is certified to the ISO27001 Standard, which regulates ""Clock synchronization"" (ISO 27001:2013, Annex A.14.4.4). Google uses a syncronized time-service protocol to ensure all systems have a common time reference. Google makes their NTP protocol public as well for use by customers. https://developers.google.com/time/	· ISO 27001 2013, Annex A.14.4.4
280	3.Technical measures	3.4. Acquisition and inspection of logs	③Syncronizing the clock to standard time	③-3	Synchronize the time of the medical information system with standard time or time information equivalent to it, provided by a trusted institution daily or more frequently in order to ensure the reliability of the time of the log.	Google is certified to the ISO27001 Standard, which regulates "Clock synchronization" (ISO 27001:2013, Annex A.14.4.4). Google uses a syncronized time-service protocol to ensure all systems have a common time reference. Google makes their NTP protocol public as well for use by customers. https://developers.google.com/time/	· ISO 27001 2013, Annex A.12.4.4
281	3.Technical measures	3.4. Acquisition and inspection of logs	④Prevention of unauthorized access in remote maintenance and acquisition and inspection of logs	④-1	Prepare procedures for remote maintenance and safety management to prevent unauthorized access to medical information systems.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google has implemented monitoring tools to detect and report application vulnerabilities. Google also maintains user access logs for privileged access and for access to user data. Logical access to audit logs is restricted to authorized personnel.	· ISO 27001 2013, Annex A.9

282	3.Technical measures	3.4. Acquisition and inspection of logs	④Prevention of unauthorized access in remote maintenance and acquisition and inspection of logs	④-2	Records of maintenance work by remote maintenance are obtained by access logs, etc., and the systems grip person confirms the content promptly.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google has implemented monitoring tools to detect and report application vulnerabilities. Google also maintains user access logs for privileged access and for access to user data. Logical access to audit logs is restricted to authorized personnel.	· ISO 27001 2013, Annex A.9
283	3.Technical measures	3.4. Acquisition and inspection of logs	④Prevention of unauthorized access in remote maintenance and acquisition and inspection of logs	④-3	When the maintenance of the information system, necessary for the service provision, is performed by remote maintenance, agree with the medical institution.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google has implemented monitoring tools to detect and report application vulnerabilities. Google also maintains user access logs for privileged access and for access to user data. Logical access to audit logs is restricted to authorized personnel.	· ISO 27001 2013, Annex A.9
284	3.Technical measures	3.4. Acquisition and inspection of logs	⑤Setting the storage period for logs in accordance with legal storage period of used medical information	⑤-1	In case of dealing medical information with statutory retention period, a longer period is set up for logs for medical record or record that can alternate it.	Not applicable. This is the customer’s responsibility to respond to.	-
285	3.Technical measures	3.4. Acquisition and	⑤Setting the storage period for	⑤-2	Agree with medical institutions on the retention period of medical information for which the statutory retention period has elapsed and medical information for which the legal retention period has not been set. The	Not applicable. This is the customer’s responsibility to respond to.	-

		inspection of logs	logs in accordance with legal storage period of used medical information		management method of logs in this section shall be handled in accordance with medical information that has a statutory retention period in principle when a retention period is set.		
286	3.Technical measures	3.5. Measures for unauthorized programs	①Installation and Management of anti-malware software	①-1	Collect information on the latest threats, check the extent of malicious code protection software installed, and confirm that there is no leakage of protection. Examples of threats to be addressed include computer viruses (worms), backdoors (Trojan horses), spyware (keyloggers), bot programs (downloaders), etc.	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001:2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/.	· ISO 27001 2013, Annex A.12.2
287	3.Technical measures	3.5. Measures for unauthorized programs	①Installation and Management of anti-malware software	①-2	The following settings are made in malicious code protection software. ・ Real-time scan (disk read/write, network communication) ・ Periodically scan if necessary as a result of risk assessment ・ On-demand scan/definition files when writing/reading data to/from electronic media, automatic updating of scan engines, manual updating with adequate frequency, prohibition of setting changes and uninstallation by anyone other than management people	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001:2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/.	· ISO 27001 2013, Annex A.12.2
288	3.Technical measures	3.5. Measures for unauthori	①Installation and Management of	①-3	When malicious codes have not been checked for a certain period of time, or when definition files or devices whose scan engines have not been updated have been checked, measures must be taken, such as	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001:2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report.	· ISO 27001 2013, Annex A.12.2

		zed programs	anti-malware software		displaying warning messages to users, notifying management users, and prohibiting or quarantining intra-facility networking.	Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/.	
289	3.Technical measures	3.5. Measures for unauthorized programs	①Installation and Management of anti-malware software	①-4	When constructing an information system, establish procedures to prevent malicious program from being mixed, and construct the system based on the procedures.	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001:2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/.	· ISO 27001 2013, Annex A.12.2
290	3.Technical measures	3.5. Measures for unauthorized programs	①Installation and Management of anti-malware software	①-5	Always update the pattern definition file of the anti-virus software to the latest one.	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001:2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/.	· ISO 27001 2013, Annex A.12.2
291	3.Technical measures	3.5. Measures for unauthori	①Installation and Management of	①-6	When constructing a medical information system, the latest anti-malware software needs to be installed in advance, in case of transplanting or downloading programs from outside. In addition, considering the	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001:2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report.	· ISO 27001 2013, Annex A.12.2

		zed programs	anti-malware software		impact on the information system, the latest security patches need to be applied.	Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/.	
292	3.Technical measures	3.5. Measures for unauthorized programs	①Installation and Management of anti-malware software	①-7	When the medical information system use environment is attacked by a virus, the medical institutions are promptly informed of the effects of the medical information system provision, and the necessary response is requested.	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001:2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/.	· ISO 27001 2013, Annex A.12.2
293	3.Technical measures	3.6. Hardening of the device and server	①Hardening of the device and server	①-1	Medical information should be saved only in the server device, and should not be saved on the terminal except for temporary storage for display.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer’s data from that of other customers and users, even when it’s stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. An employee’s authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and Google Workspace products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Google's Terms of Service covers the process for accessing Customer Data (5.2 Protection of Customer Data) which mentions: Google will only access or use Customer Data to provide the Services and Technical Support Service (TSS) to Customer or as otherwise instructed by Customer	· ISO 27001 2013, Annex A.9

						and will not use it for any other Google products, services, or advertising. Google has implemented and will maintain administrative, physical, and technical safeguards to protect Customer Data, as further described in the Data Processing and Security Terms. Google proprietary event management tool is used by the Security Team to monitor traffic between sites and send alerts when suspicious behavior is detected. Google also has direct monitoring of certain important data sources such as source code. Note that transfer of large amounts of data between the corporate and production networks is quite routine and is not itself cause for an alert; however, a large transfer to an external location such as an external storage cloud, or access to source code from an unexpected IP address would likely be detected and cause an alert to be generated. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	
294	3.Technical measures	3.6. Hardening of the device and server	①Hardening of the device and server	①-2	Restrict the servers to which web browsers connect to servers that are required for business.	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001:2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/. Google routes ingress and egress traffic through proprietary boundary devices that, among other functions, act as proxy servers between user terminals and Google's internal network. The use of these boundary devices prevent direct connections between Google's internal and external networks and allows for obfuscation of internal network identifiers and configuration, load balancing, traffic filtering, and efficient routing of user requests.	· ISO 27001 2013, Annex A.12.2
295	3.Technical measures	3.6. Hardening of the device and server	①Hardening of the device and server	①-3	The web browser must be configured to not allow code to be downloaded and executed from unauthorized sites, such as ActiveX, applets for Java, or Flash (only servers on which management software is executed).	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001:2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows	· ISO 27001 2013, Annex A.12.2

						up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/. Google has issued implementation guidance documented in policy and procedures that restricts the use of software and services that expose the information system to unacceptable risk. The Google Security team detects and blocks harmful vulnerabilities within Google's system to protect Google from compromise. Google maintains a list of applications (e.g., Adobe Flash Player, Java browser plugin) that have been blocked due to security flaws within the applications.	
296	3.Technical measures	3.6. Hardening of the device and server	①Hardening of the device and server	①-4	Code downloaded from authorized sites should also be checked by anti-malware software.	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001:2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/.	· ISO 27001 2013, Annex A.12.2
297	3.Technical measures	3.6. Hardening of the device and server	①Hardening of the device and server	①-5	It is desirable to perform setting so that an external application which is not assumed in a business process of a mail client or the like is not activated from a web browser without explicit confirmation.	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001:2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/.	· ISO 27001 2013, Annex A.12.2
298	3.Technical measures	3.6. Hardening of the device	①Hardening of the device	①-6	An appropriate upper limit should be set for the number of simultaneous logon users (OS accounts, etc.) to servers, etc. of medical-information systems.	Google is certified to the ISO27001 Standard, which regulates "Access to Networks and Network Services" (ISO27001:2013, Annex A.9.1.2), "Network Security Management" (ISO27001:2013, Annex A.13.1).	· ISO 27001 2013, Annex A.9.1.2,13.1

		and server	and server			We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately.	
299	3.Technical measures	3.6. Hardening of the device and server	①Hardening of the device and server	①-7	Do not install unnecessary applications on devices used in medical information systems.	Google is certified to the ISO27001 Standard, which regulates "Restrictions on software installation" (ISO 27001:2013, Annex A.12.6). Google prevents program execution in accordance with approved machine distributions and software binaries list. Google denies non-standard distributions from running on machine. A set of proprietary configuration management tools synchronize system files on the root partition across all production machines with the standard and approved configuration in the version control system. The tools checks the machine for deviations and corrects these deviations throughout the day. Automated verification software that runs in production detects software binaries, which have not been released through approved channels.	· ISO 27001 2013, Annex A. 12.6
300	3.Technical measures	3.6. Hardening of the device and server	①Hardening of the device and server	①-8	In case of taking a device storing information related to medical information systems, install only a minimum number of applications necessary for the purpose.	Not applicable. This is the customer’s responsibility to respond to.	-
301	3.Technical measures	3.6. Hardening of the device and server	①Hardening of the device and server	①-9	Determine the procedure for application installation when taking out device that stores information about the medical information system.	Not applicable. This is the customer’s responsibility to respond to.	-
302	3.Technical measures	3.7. Measures for vulnerability of	①Use of the network device which the	①-1	For network devices such as routers, use devices whose safety can be checked.	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A.11.2).	· ISO 27001 2013, Annex A.11.2

		devices and software	safety is confirmed			Google maintains security configurations for its machines and network devices. The configurations are maintained and serve as master copies for comparision against production instances. Deviations are identified and corrected.	
303	3.Technical measures	3.7. Measures for vulnerability of devices and software	①Use of the network device which the safety is confirmed	①-2	Network devices, such as routers, select security targets or similar documents defined in the ISO15408 that conform to this guideline.	Google is certified to the ISO27001 Standard, which regulates "Documented Operating Procedures" (ISO27001:2013, Annex A.12.1.1). Google maintains robust internal documentation and maintains an ISMS, per ISO27001 requirements. All documentation in on systems that are replicated and subject to backup. Customers using Google Cloud Platform, retain all rights and responsibilities to configure and manage their environment, including development of operational guidance. Google ensures all hardware and network devices are evaluated before purchase. All critical components are developed by Google in accordance with proprietary standards and highly customized features that are not commercially available. As a result, Common Criteria evaluations cannot be applied to Google's hardware and software. Instead Google relies on the internal security reviews for testing of acquires systems and services.	· ISO 27001 2013, Annex A.12.1.1
304	3.Technical measures	3.7. Measures for vulnerability of devices and software	②Performance of patch application	②-1	Management technical vulnerabilities related to medical-information systems using a ledger, etc.	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001:2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/.	· ISO 27001 2013, Annex A.12.2
305	3.Technical measures	3.7. Measures for vulnerability of devices and software	②Performance of patch application	②-2	If potential technical vulnerabilities are identified, perform risk analysis and determine the necessary actions (patch application, configuration change, etc.).	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001:2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains	· ISO 27001 2013, Annex A.12.2

						relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/.	
306	3.Technical measures	3.7. Measures for vulnerability of devices and software	②Performance of patch application	②-3	Verify that the patch has not been tampered with and is valid before applying the patch.	Google is certified to the ISO27001 Standard, which regulates "Change Management" (ISO27001:2013 Annex A 12.1.2) and "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14). Please see the Google Infrastructure Security Design Overview - https://cloud.google.com/security/security-design/ for more details. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including change management and system development procedures.	· ISO 27001 2013, Annex A.12.1.2,14
307	3.Technical measures	3.7. Measures for vulnerability of devices and software	②Performance of patch application	②-4	When upgrading the operating system and applying security patches, evaluate the impact on medical information systems and check the test results before performing the upgrade.	Google is certified to the ISO27001 Standard, which regulates "Separation of Development, Testing, and Operational Environments" (ISO 27001:2013, Annex A.12.1.4), " and Security in Development and Support Processes" (ISO 27001:2013, Annex A.14.2). Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	· ISO 27001 2013, Annex A.12.1.2,14
308	3.Technical measures	3.7. Measures for vulnerability of devices and software	③Performance of vulnerability inspection to medical information system	③-1	Regarding the applications to be provided, safety diagnostics including specific vulnerability detection by application type should be performed periodically, and measures should be taken based on the results. Introduce mechanisms to verify the integrity of data when sending and receiving data to and from healthcare institutions.	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" ISO 27001:2013, (Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/. Within Google, members of the information security team review security plans for all networks, systems and services. They provide project-specific consulting services to Google’s product and engineering teams. They monitor for suspicious activity on Google’s networks, address information security threats, perform routine security evaluations and audits, and engage outside experts to conduct regular security assessments. We specifically built a full-time team, known as Project Zero, that aims to prevent targeted attacks by reporting bugs to software vendors and filing them in an external database.	· ISO 27001 2013, Annex A.12.2

Guidelines for Safety Management of Medical Information by Providers of Information Systems and Services Handling Medical Information

Handbook for Google Cloud and Google Workspace

309	3.Technical measures	3.7. Measures for vulnerability of devices and software	③Performance of vulnerability inspection to medical information system	③-2	It is preferable that the safety diagnostic of the application is not performed directly on the provided service, but is performed by preparing a test environment separately.	Google is certified to the ISO27001 Standard, which regulates "Separation of Development, Testing, and Operational Environments" (ISO 27001:2013, Annex A.12.1.4), " and Security in Development and Support Processes" (ISO 27001:2013, Annex A.14.2). Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	· ISO 27001 2013, Annex A.12.1.2,14
310	3.Technical measures	3.7. Measures for vulnerability of devices and software	③Performance of vulnerability inspection to medical information system	③-3	It is desirable to perform vulnerability detection of developed software at the source code level. When it is impossible to request the provision of source code such as package software, the application is operated instead of the source code level, and the external vulnerability check is performed.	Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14). Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including managing their system development process.	· ISO 27001 2013, Annex A.14
311	3.Technical measures	3.7. Measures for vulnerability of devices and software	④Gathering information of latest vulnerability	④-1	For applications and third-party software (libraries, server processes, etc.) to be used for application operation, refer to the latest vulnerability information to be disclosed and take prompt measures.	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001:2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/.	· ISO 27001 2013, Annex A.12.2
312	3.Technical measures	3.7. Measures for vulnerability of devices and software	④Gathering information of latest vulnerability	④-2	Information on vulnerabilities of medical information systems is acquired and verified regularly at the required timing, from information sources such as JPCERT Coordination Center (JPCERT/CC), the Cabinet Cyber Security Center (NISC), and the Institute for Information Processing of Independent Administrative Organizations (IPA).	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001:2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues	· ISO 27001 2013, Annex A.12.2

						in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/.	
313	3.Technical measures	3.7. Measures for vulnerability of devices and software	⑤gathering information and responding to vulnerability related to IoT devices	⑤-1	When providing services including the use of IoT devices, agree with medical institutions on the responsibility division with medical institutions.	Not applicable. This is the customer's responsibility to respond to.	-
314	3.Technical measures	3.7. Measures for vulnerability of devices and software	⑤gathering information and responding to vulnerability related to IoT devices	⑤-2	When services including the use of IoT equipments are provided, information on vulnerabilities to the IoT devices expected to be used is periodically collected and necessary measures are taken.	Not applicable. This is the customer's responsibility to respond to.	-
315	3.Technical measures	3.8. Access restriction on the network	①Access restriction of network	①-1	Provide security gateways (firewalls, routers, etc. installed at network boundaries) to control access to each network interface based on established policies, such as restricting connection destinations and restricting connection times. When a security gateway cannot be installed at a network boundary at the time of using hosting, the same access control shall be performed by individual information processing apparatuses (servers).	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A.11.2). Google maintains security configurations for its machines and network devices. The configurations are maintained and serve as master copies for comparision against production instances. Deviations are identified and corrected.	· ISO 27001 2013, Annex A.11.2
316	3.Technical measures	3.8. Access restriction on the network	①Access restriction of network	①-2	In the security gateway, setting is made so that traffic having an unauthorized IP address cannot pass through (by setting the IP address of a connection device or the like as a private address, and controlling traffic to pass through the security gateway such as a firewall or a VPN device on the basis of the IP address).	Google is certified to the ISO27001 Standard, which regulates "Communications Security" (ISO 27001:2013, Annex A.13), and "Securing Application Service on Public Networks" ISO 27001:2013, (Annex A.14.1.2). Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including management of external connections.	· ISO 27001 2013, Annex A.13,14.1.2
317	3.Technical measures	3.8. Access restriction	①Access restriction of network	①-3	In medical information systems, connection to services on open networks such as the Internet should be limited to the following services.	Google is certified to the ISO27001 Standard, which regulates "Communications Security" (ISO 27001:2013, Annex A.13), and "Securing Application Service on Public Networks" ISO 27001:2013, (Annex A.14.1.2).	· ISO 27001 2013, Annex A.13,14.1.2

		on the network			If there are other necessary services, use them after obtaining agreement from medical institutions, etc. ・ Use monitoring and remote maintenance of medical information systems from outside ・ Download of the latest pattern file of security software ・ Downloading security patch files for operating systems and applications ・ Access to the time authentication authority at the time of electronic signature, and access to the certificate authority such as a lapse list at the time of electronic signature verification ・ Monitoring unauthorized access to security devices such as firewalls, IDS and IPS ・ Accessing a Time Distribution Server for Time Synchronization ・ Internet services (e.g., access to domain name servers) required to use these services ・ Other services necessary for the operation of medical information systems (external authentication server, external medical information database, etc.)	Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including management of external connections.	
318	3.Technical measures	3.8. Access restriction on the network	②Prevention of impersonation	②-1	The following items should be agreed in advance for information exchange. ・ Procedures for recording and exchanging information on electronic media ・ Procedure for exchanging information in document file format via network ・ Procedure for exchanging information with application input via network ・ Method and verification procedure for attaching an electronic signature and a time stamp to information	Not applicable. This is the customer's responsibility to respond to.	-
319	3.Technical measures	3.8. Access restriction on the network	②Prevention of impersonation	②-2	In the information exchange procedure, the following items should be ensured regardless of the form of transport. ・ Identify and record senders and recipients. ・ Prevent non-repudiation measures, such as saving shipping slips, giving electronic signatures to document files, and reliably authenticating applications when logging on, so that senders' activities cannot be denied later. ・ Agree on the confidentiality level of the information to be exchanged (not lowering the confidentiality level at the recipient).	Google is certified to the ISO27001 Standard, which regulates "Cryptography" (ISO 27001:2013, Annex A.10) Encryption is used to protect user authentication and administrator sessions transmitted over the Internet. Remote access to Google corporate machines requires a Google issued digital certificate installed on the connecting device and two-factor authentication. Google publishes details about encryption and key management options for its Google Cloud Platform and Google Workspace products. To read more about key management and encryption, please see: https://cloud.google.com/security/encryption-at-rest/ https://cloud.google.com/security/encryption-in-transit/ https://services.google.com/fh/files/misc/google-workspace-encryption-wp.pdf	· ISO 27001 2013, Annex A.10

					・ Ensure that the exchanged information does not contain malicious code.	Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including development of appropriate encryption measures.	
320	3.Technical measures	3.8. Access restriction on the network	②Prevention of impersonation	②-3	The following measures should be taken when electronically transferring datum. ・ The sender and the recipients must authenticate each other electronically to verify the validity of the other party. Although the authentication method varies depending on the connection mode and the application used for transfer, it is desirable to authenticate the equipments and the users. ・ The transmission and reception paths should be protected from the risk of interception in an appropriate way. ・ Measures should be taken to verify that the received information is not damaged or tampered on the way. ・ When transmission and reception fail, retransmission and reception should be attempted with a predefined number of times as an upper limit. When the upper limit is reached, all communication between the sender and receiver should be stopped, and work such as specifying a disability should be performed.	Google is certified to the ISO27001 Standard, which regulates "Cryptography" (ISO 27001:2013, Annex A.10) Encryption is used to protect user authentication and administrator sessions transmitted over the Internet. Remote access to Google corporate machines requires a Google issued digital certificate installed on the connecting device and two-factor authentication. Google publishes details about encryption and key management options for its Google Cloud Platform and Google Workspace products. To read more about key management and encryption, please see: https://cloud.google.com/security/encryption-at-rest/ https://cloud.google.com/security/encryption-in-transit/ https://services.google.com/fh/files/misc/google-workspace-encryption-wp.pdf Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including development of appropriate encryption measures.	· ISO 27001 2013, Annex A.10
321	3.Technical measures	3.8. Access restriction on the network	②Prevention of impersonation	②-4	In the network from medical institutions to the contractor, the route is confirmed by the entrance and exit, the used equipment, the functional unit on the used equipment, and the necessary unit of the user at the base of transmission/reception of the medical institution.	Google's security teams are committed to a strong perimeter and dedicated staff are responsible for the safety and security of Google's network infrastructure. Google conducts rigorous internal continuous testing of our network perimeter through various types of penetration exercises. In addition, Google coordinates external third party penetration testing using qualified and certified penetration testers.	-
322	3.Technical measures	3.8. Access restriction on the network	②Prevention of impersonation	②-5	In ②-4, mutual authentication is performed between a server externally connected by a medical institution and a server of contractor.	Google's security teams are committed to a strong perimeter and dedicated staff are responsible for the safety and security of Google's network infrastructure. Google conducts rigorous internal continuous testing of our network perimeter through various types of penetration exercises. In addition, Google coordinates external third party penetration testing using qualified and certified penetration testers.	-
323	3.Technical measures	3.8. Access restriction on the network	②Prevention of impersonation	②-6	Regarding ②-4, if the contractor re-entrusts the maintenance operation, measures are taken to prevent spoofing separately for the connection between the contractor and the re-entrusted destination.	Google's security teams are committed to a strong perimeter and dedicated staff are responsible for the safety and security of Google's network infrastructure. Google conducts rigorous internal continuous testing of our network perimeter through various types of penetration exercises. In addition, Google coordinates external third party penetration testing using qualified and certified penetration testers.	-
324	3.Technical measures	3.8. Access	②Prevention of	②-7	Agree with the Medical Institute, to verify the validity of the means of authentication for communication method	Google's security teams are committed to a strong perimeter and dedicated staff are responsible for the safety and security of Google's network infrastructure.	-

		restriction on the network	imperson ation		adopted by the Medical Institute, based on 2 in Section 6.11 C of the Fifth Edition of the Health, Labor and Health Department Guidelines.	Google conducts rigorous internal continuous testing of our network perimeter through various types of penetration exercises. In addition, Google coordinates external third party penetration testing using qualified and certified penetration testers.	
325	3.Technical measures	3.8. Access restriction on the network	③Access restriction of unauthori zed devices to the network port	③-1	Restrict physical connection of network devices, servers, and terminals to unused network ports.	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A.11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers	· ISO 27001 2013, Annex A.11.2
326	3.Technical measures	3.8. Access restriction on the network	③Access restriction of unauthori zed devices to the network port	③-2	To Identify unauthorized devices, create and maintain a list of information processing devices used in medical information systems.	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001:2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	· ISO 27001 2013, Annex A.8.1,8.3.2,11.2.7,12.5

327	3.Technical measures	3.8. Access restriction on the network	③Access restriction of unauthorized devices to the network port	③-3	In order to avoid adverse effects of an unauthorized information processing apparatus being connected to a network, a mechanism for checking consistency with a registered network address, that a malicious program has not been infected, that a vulnerability patch has been applied, and the like before connection should be established and operated.	Google is certified to the ISO27001 Standard, which regulates "Logging and Monitoring" (ISO 27001:2013, Annex A.12.4). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's security monitoring program is focused on information gathered from internal network traffic, employee actions on systems and outside knowledge of vulnerabilities. At many points across our global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. This analysis is performed using a combination of open-source and commercial tools for traffic capture and parsing. A proprietary correlation system built on top of Google technology also supports this analysis. Network analysis is supplemented by examining system logs to identify unusual behavior, such as attempted access of customer data. Google security engineers place standing search alerts on public data repositories to look for security incidents that might affect the company's infrastructure. They actively review inbound security reports and monitor public mailing lists, blog posts, and wikis. Automated network analysis helps determine when an unknown threat may exist and escalates to Google security staff, and network analysis is supplemented by automated analysis of system logs. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuration of specific monitoring to detect false or unverified data.	· ISO 27001 2013, Annex A.12.4
328	3.Technical measures	3.8. Access restriction on the network	④Measures when using wireless LAN	④-1	For security measures necessary when medical institutions use wireless LANs when using services that handle medical information, agree with medical institutions on roles sharing between contractor.	Not applicable. This is the customer's responsibility to respond to.	-
329	3.Technical measures	3.8. Access restriction on the network	④Measures when using wireless LAN	④-2	In business, when a mobile terminal storing information on a service is taken out, connection to a public wireless LAN is not performed.	Not applicable. This is the customer's responsibility to respond to.	-
330	3.Technical measures	3.9. Detection and block of unauthorized communication	①Detection and block of unauthorized communication	①-1	An intrusion detection system (IDS), an intrusion prevention system (IPS) and the like are introduced at the boundary of a network connected to medical institutions and the like to detect an unauthorized event on the network, or to block unauthorized traffic. When a device cannot be installed at a network boundary, such as when hosting is used, the same control is performed in each information processing apparatus.	Google has implemented network and host base tools to detect and respond to potential security incidents. Google maintains automated log collection and analysis tools to support investigations.	-
331	3.Technical measures	3.9. Detection and block of unauthori	①Detection and block of unauthorized	①-2	Updating of signature/detection rules and application of software-security patches should be carried out so that intrusion detection systems can cope with newest hit and unauthorized accesses at all times.	Google is certified to the ISO27001 Standard, which regulates "Access to Networks and Network Services" (ISO27001:2013, Annex A.9.1.2), "Network Security Management" (ISO27001:2013, Annex A.13.1).	· ISO 27001 2013, Annex A.9.1.2,13.1

		zed communication	communication			We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately.	
332	3.Technical measures	3.9. Detection and block of unauthorized communication	①Detection and block of unauthorized communication	①-3	When intrusion detection systems detect urgent hit or unauthorized access, they must immediately notify the management personnel by outputting to the monitoring terminal or by e-mail.	Google is certified to the ISO27001 Standard, which regulates "Access to Networks and Network Services" (ISO27001:2013, Annex A.9.1.2), "Network Security Management" (ISO27001:2013, Annex A.13.1). We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately.	· ISO 27001 2013, Annex A.9.1.2,13.1
333	3.Technical measures	3.9. Detection and block of unauthorized communication	①Detection and block of unauthorized communication	①-4	The record of intrusion detection includes items necessary for post-processing such as unauthorized access.	Google is certified to the ISO27001 Standard, which regulates "Access to Networks and Network Services" (ISO27001:2013, Annex A.9.1.2), "Network Controls" (ISO27001:2013, Annex A.13.1.1). We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help	· ISO 27001 2013, Annex A.9.1.2,13.1

						ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately.	
334	3.Technical measures	3.9. Detection and block of unauthorized communication	①Detection and block of unauthorized communication	①-5	It is desirable to monitor at the network boundary that fraud and suspicious traffic is not flowing from the medical information system from the internal network to the external network.	Google is certified to the ISO27001 Standard, which regulates "Logging and Monitoring" (ISO 27001:2013, Annex A.12.4). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's security monitoring program is focused on information gathered from internal network traffic, employee actions on systems and outside knowledge of vulnerabilities. At many points across our global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. This analysis is performed using a combination of open-source and commercial tools for traffic capture and parsing. A proprietary correlation system built on top of Google technology also supports this analysis. Network analysis is supplemented by examining system logs to identify unusual behavior, such as attempted access of customer data. Google security engineers place standing search alerts on public data repositories to look for security incidents that might affect the company's infrastructure. They actively review inbound security reports and monitor public mailing lists, blog posts, and wikis. Automated network analysis helps determine when an unknown threat may exist and escalates to Google security staff, and network analysis is supplemented by automated analysis of system logs. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuration of specific monitoring to detect false or unverified data.	· ISO 27001 2013, Annex A.12.4
335	3.Technical measures	3.9. Detection and block of unauthorized communication	①Detection and block of unauthorized communication	①-6	It is desirable that the intrusion detection system itself be set so as not to be subject to hit and unauthorized access (stealth mode), and that the access to the intrusion detection system be appropriately controlled.	Google is certified to the ISO27001 Standard, which regulates "Access to Networks and Network Services" (ISO27001:2013, Annex A.9.1.2), "Network Security Management" (ISO27001:2013, Annex A.13.1). We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team.	· ISO 27001 2013, Annex A.9.1.2, 13.1

						Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately.	
336	3.Technical measures	3.9. Detection and block of unauthorized communication	①Detection and block of unauthorized communication	①-7	When a service including the use of an IoT equipment is provided, the state of access to the medical information system by the IoT device is recorded, and the absence of unauthorized access is periodically monitored.	Not applicable. This is the customer's responsibility to respond to.	-
337	3.Technical measures	3.10. Management of device and data to be carried out	①Authentication of devices to be carried out	①-1	Set a startup password for devices.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and Google Workspace products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Google's Terms of Service covers the process for accessing Customer Data (5.2 Protection of Customer Data): Google will only access or use Customer Data to provide the Services and Technical Support Service (TSS) to Customer or as otherwise instructed by Customer and will not use it for any other Google products, services, or advertising. Google has implemented and will maintain administrative, physical, and technical safeguards to protect Customer Data, as further described in the Data Processing and Security Terms. The Google Security Team establishes usage restrictions, connection requirements, configuration requirements, and implementation guidance for mobile devices. Google has identified multiple trust tiers for mobile devices. Only devices classified as Highly Privileged Access are permitted access to the production environment. Google issued machine certificates are required to be installed on all devices that connect to the production environment. Google's network infrastructure validates the machine certificates and denies access to machines without a valid certificate. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies.	· ISO 27001 2013, Annex A.9

						Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	
338	3.Technical measures	3.10. Management of device and data to be carried out	①Authentication of devices to be carried out	①-2	Measures should be taken to prevent an unauthorized activation of a device by a third party, such as setting an activation password that is hard to guess and periodically changing the activation password according to the characteristics of the device.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and Google Workspace products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Google's Terms of Service covers the process for accessing Customer Data (5.2 Protection of Customer Data): Google will only access or use Customer Data to provide the Services and Technical Support Service (TSS) to Customer or as otherwise instructed by Customer and will not use it for any other Google products, services, or advertising. Google has implemented and will maintain administrative, physical, and technical safeguards to protect Customer Data, as further described in the Data Processing and Security Terms. The Google Security Team establishes usage restrictions, connection requirements, configuration requirements, and implementation guidance for mobile devices. Google has identified multiple trust tiers for mobile devices. Only devices classified as Highly Privileged Access are permitted access to the production environment. Google issued machine certificates are required to be installed on all devices that connect to the production environment. Google's network infrastructure validates the machine certificates and denies access to machines without a valid certificate. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	· ISO 27001 2013, Annex A.9
339	3.Technical measures	3.10. Management of device	①Authentication of devices to	①-3	A plurality of authentication elements are combined for login and access to an information device that stores information related to a medical information system.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9).	· ISO 27001 2013, Annex A.9

		and data to be carried out	be carried out			Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud Platform and Google Workspace products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Google's Terms of Service covers the process for accessing Customer Data (5.2 Protection of Customer Data): Google will only access or use Customer Data to provide the Services and Technical Support Service (TSS) to Customer or as otherwise instructed by Customer and will not use it for any other Google products, services, or advertising. Google has implemented and will maintain administrative, physical, and technical safeguards to protect Customer Data, as further described in the Data Processing and Security Terms. The Google Security Team establishes usage restrictions, connection requirements, configuration requirements, and implementation guidance for mobile devices. Google has identified multiple trust tiers for mobile devices. Only devices classified as Highly Privileged Access are permitted access to the production environment. Google issued machine certificates are required to be installed on all devices that connect to the production environment. Google's network infrastructure validates the machine certificates and denies access to machines without a valid certificate. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	
340	3.Technical measures	3.10. Management of device and data to be carried out	②Measures for information to be carried out	②-1	Procedure for taking out devices or media storing information, includes encrypting the devices or media itself, encrypting the stored information, and setting passwords.	Google is certified to the ISO27001 Standard, which regulates "Cryptography" (ISO 27001:2013, Annex A.10) Customer data that is uploaded or created is encrypted at rest. We use several layers of encryption to protect customer data; adding redundant data protection and allowing us to select the optimal approach based on application requirements. Google publishes details about encryption and key management options for its Google Cloud Platform and Google Workspace products. To read more about key management and encryption, please see: https://cloud.google.com/security/encryption-at-rest/ https://services.google.com/fh/files/misc/google-workspace-encryption-wp.pdf	· ISO 27001 2013, Annex A10

						Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including development of appropriate encryption measures.	
341	3.Technical measures	3.11. Measures for data leakage by desktop virtualization, MDM and MAM	①Management of devices owned by individual	①-1	Agree with the medical institution on countermeasures against the use of the medical information system by user's privately owned devices. Furthermore, refer to the below for specific details. ・ In order to prevent leakage of information from equipments owned by users, for example, it is conceivable to divide business use areas and personal use areas at the OS-level using virtual desktops so that medical institutions and others can grip the business use areas. In addition, mobile device management (MDM) and mobile application management (MAM) can be applied to strictly implement security measures equivalent to security measures for terminals owned by medical institutions and others, which are owned and managed by medical institutions and others.	Employees are provided Google machines and mobile devices for business use. Additionally, Google allows Google-managed, user-owned devices for business use. Such devices are fully managed by Google.	-
342	3.Technical measures	3.11. Measures for data leakage by desktop virtualization, MDM and MAM	①Management of devices owned by individual	①-2	In principle, the use of employee-owned devices for purposes related to the provision of services (development, repair and operation) is prohibited.	Employees are provided Google machines and mobile devices for business use. Additionally, Google allows Google-managed, user-owned devices for business use. Such devices are fully managed by Google.	-
343	3.Technical measures	3.11. Measures for data leakage by desktop virtualization, MDM and MAM	②Implementation of technology that does not leave data on the device	②-1	When a user of a medical institution uses a service outside the medical institution, an agreement is made with the medical institution in sharing the role of the entrusted business operator to introduce the technology of virtual desktop into the working environment of the computer used by the user of the medical institution.	Not applicable. This is the customer’s responsibility to respond to.	-
344	3.Technical measures	3.12. Access restriction of unregistered	①Connection Restriction of unregistered	①-1	In the medical information system, unnecessary device drivers are removed to limit the type of electronic media that can access the server. In addition, to prevent unauthorized types of devices from being connected, it is advisable to make a setting	Google is certified to the ISO27001 and ISO27017 Standards, which regulates "Access Control" (ISO 27001:2013, Annex A.9), "Change Management" (ISO 27001:2013, Annex 12.1.2), "Virtual Machine (Hardening)" (ISO 27017:2015, Annex A.CLD.9.4.2).	ISO 27001:2013, Annex A.9,12.1.2 ISO 27017:2015, Annex A.CLD.9.4.2

		electronic devices	electronic media to servers		that prevents the installation or uninstallation of device drivers other than the administrator.	Information security oversight and management controls, including logical access and change management controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google uses devices that have been heavily customized, and uses operating systems and configurations that have been modified from factory standard to eliminate unnecessary features, ports, etc. Google system engineers create custom configurations that increase security and significantly reduce the attack vectors for their devices. Tools are also utilized to detect deviations from pre-defined Operating System (OS) configurations on production machines and correct them automatically. This allows for an easy roll out of updates to system files in a consistent manner and helps ensure that machines are automatically updated.	
345	3.Technical measures	3.12. Access restriction of unregistered electronic devices	①Connection Restriction of unregistered electronic media to servers	①-2	It is desirable to periodically verify that no unnecessary device driver has been added.	Google is certified to the ISO27001 and ISO27017 Standards, which regulates "Access Control" (ISO 27001:2013, Annex A.9), "Change Management" (ISO 27001:2013, Annex 12.1.2), "Virtual Machine (Hardening)" (ISO 27017:2015, Annex A.CLD.9.4.2). Information security oversight and management controls, including logical access and change management controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google uses devices that have been heavily customized, and uses operating systems and configurations that have been modified from factory standard to eliminate unnecessary features, ports, etc. Google system engineers create custom configurations that increase security and significantly reduce the attack vectors for their devices. Tools are also utilized to detect deviations from pre-defined Operating System (OS) configurations on production machines and correct them automatically. This allows for an easy roll out of updates to system files in a consistent manner and helps ensure that machines are automatically updated.	ISO 27001:2013, Annex A.9,12.1.2 ISO 27017:2015, Annex A.CLD.9.4.2
346	3.Technical measures	3.13. Use of encryption and electronic signature	①Use of secure encryption and electronic signature	①-1	In the network, measures necessary to protect information from eavesdropping, tampering, communication through wrong routes, destruction, and the like (maintenance of implementation standards and procedures of information exchange, encryption of communication, and the like) are performed.	Google is certified to the ISO27001 Standard, which regulates "Cryptographic controls" and "13.1 Network security management" (ISO27001:2013, Annex A.10.1, 13.1). Controls relating to Network Architecture and Management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. Please see https://cloud.google.com/security/encryption-in-transit/ for more informaiton.	· ISO 27001 2013, Annex A.10.1, 13.1

347	3.Technical measures	3.13. Use of encryption and electronic signature	①Use of secure encryption and electronic signature	①-2	Take necessary measures (implementation of a server certificate, etc.) to prevent access destination spoofing (session hijacking, phishing, etc.).	Google is certified to the ISO27001 Standard, which regulates "Cryptographic controls" and "13.1 Network security management" (ISO27001:2013, Annex A.10.1, 13.1). Controls relating to Network Architecture and Management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. Please see https://cloud.google.com/security/encryption-in-transit/ for more informaiton.	· ISO 27001 2013, Annex A.10.1, 13.1
348	3.Technical measures	3.13. Use of encryption and electronic signature	①Use of secure encryption and electronic signature	①-3	To ensure route security, agree with medical institutions on IPsec+IKE and closed network and its' conditions.	Google is certified to the ISO27001 Standard, which regulates "Cryptographic controls" and "13.1 Network security management" (ISO27001:2013, Annex A.10.1, 13.1). Controls relating to Network Architecture and Management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. Please see https://cloud.google.com/security/encryption-in-transit/ for more informaiton.	· ISO 27001 2013, Annex A.10.1, 13.1
349	3.Technical measures	3.13. Use of encryption and electronic signature	①Use of secure encryption and electronic signature	①-4	Direct interception risks should be considered for cables used for information transmission.	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0	· ISO 27001 2013, Annex A.11

						Google adheres to all building and facility requirements in the region where its data centers are located.	
350	3.Technical measures	3.13. Use of encryption and electronic signature	①Use of secure encryption and electronic signature	①-5	Use cryptographic algorithms with sufficient security. Use e-Government Recommended Cryptography Lists as selection criteria.	Google is certified to the ISO27001 Standard, which regulates "Cryptography" (ISO 27001:2013, Annex A.10) Customer data that is uploaded or created is encrypted at rest. We use several layers of encryption to protect customer data; adding redundant data protection and allowing us to select the optimal approach based on application requirements. Google publishes details about encryption and key management options for its Google Cloud Platform and Google Workspace products. To read more about key management and encryption, please see: https://cloud.google.com/security/encryption-at-rest/ https://services.google.com/fh/files/misc/google-workspace-encryption-wp.pdf Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including development of appropriate encryption measures.	· ISO 27001 2013, Annex A.10
351	3.Technical measures	3.13. Use of encryption and electronic signature	①Use of secure encryption and electronic signature	①-6	Security measures against the information itself, such as encryption, are implemented between the transmission source and the transmission destination.	Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. Please see https://cloud.google.com/security/encryption-in-transit/ for more informaiton.	· ISO 27001 2013, Annex A.10
352	3.Technical measures	3.13. Use of encryption and electronic signature	①Use of secure encryption and electronic signature	①-7	When using the SSL/TLS to provide services, the actions described in TLS1. 2 should be taken.	Google supports the use of open encryption methodologies. Google forces TLS for all authentication traffic. Customer data is encrypted when on Google's internal networks, in transport and at rest.	· ISO 27001 2013, Annex A.10
353	3.Technical measures	3.13. Use of encryption and electronic signature	①Use of secure encryption and electronic signature	①-8	In addition to ①-7, when medical institutions request email encryption (S/MIME, etc.) or file encryption, agree with medical institutions on the measures and conditions necessary for responding.	Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. Please see https://cloud.google.com/security/encryption-in-transit/ for more informaiton.	· ISO 27001 2013, Annex A.10
354	3.Technical measures	3.13. Use of encryption and electronic signature	①Use of secure encryption and electronic signature	①-9	Follow the steps below when having a VPN connection. ・ Authentication should be mutually performed between VPN devices, when connected. ・ To minimize the risks of interception and replay, use appropriate crypto technique. ・ Do not set a direct path between the private network interface and the Internet interface to prevent traffic on the Internet from entering the VPN channel.	Google is certified to the ISO27001 Standard, which regulates "Communications Security" (ISO 27001:2013, Annex A.13), and "Securing Application Service on Public Networks" ISO 27001:2013, (Annex A.14.1.2). Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including management of external connections.	· ISO 27001 2013, Annex A.13,14.1.2

					・ Implement measures, such as establishing VPN channels for each medical institution, to avoid the risk of information confusion between medical institutions when information processing services are entrusted from multiple medical institutions.		
355	3.Technical measures	3.13. Use of encryption and electronic signature	①Use of secure encryption and electronic signature	①-10	When connecting via an open network using the HTTPS, both the server and the client set up the TLS appropriately in accordance with the "high security type" with the highest security specified in the "SSL/TLS cryptography setting guideline".	Google supports the use of open encryption methodologies. Google forces TLS for all authentication traffic. Customer data is encrypted when on Google's internal networks, in transport and at rest.	-
356	3.Technical measures	3.13. Use of encryption and electronic signature	①Use of secure encryption and electronic signature	①-11	SSL-VPN is not used in principle.	Google supports the use of open encryption methodologies. Google forces TLS for all authentication traffic. Customer data is encrypted when on Google's internal networks, in transport and at rest.	-
357	3.Technical measures	3.13. Use of encryption and electronic signature	①Use of secure encryption and electronic signature	①-12	In providing services, when connecting by software-based IPsec or TLS1. 2, appropriate measures should be taken for hit caused by looping between sessions (accessing closed sessions that are not legitimate routes).	Google supports the use of open encryption methodologies. Google forces TLS for all authentication traffic. Customer data is encrypted when on Google's internal networks, in transport and at rest.	-
358	3.Technical measures	3.13. Use of encryption and electronic signature	①Use of secure encryption and electronic signature	①-13	Provide information on appropriate countermeasures against attacks by circumvention between sessions (access to closed sessions that are not legitimate routes) when users in healthcare connect via software-type IPsec or TLS 1.2. Agree with medical institutions on the scope and conditions of information provision.	Google supports the use of open encryption methodologies. Google forces TLS for all authentication traffic. Customer data is encrypted when on Google's internal networks, in transport and at rest.	-
359	3.Technical measures	3.13. Use of encryption and electronic signature	②Managing encryption key and electronic signature to prevent the risk of encryption algorithm and	②-1	Develop countermeasures against leakage of encryption keys.	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" ISO 27001:2013, (Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues	· ISO 27001 2013, Annex A.12.2

			leakage of encryption			in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity/. Within Google, members of the information security team review security plans for all networks, systems and services. They provide project-specific consulting services to Google's product and engineering teams. They monitor for suspicious activity on Google's networks, address information security threats, perform routine security evaluations and audits, and engage outside experts to conduct regular security assessments. We specifically built a full-time team, known as Project Zero, that aims to prevent targeted attacks by reporting bugs to software vendors and filing them in an external database.	
360	3.Technical measures	3.13. Use of encryption and electronic signature	②Managing encryption key and electronic signature to prevent the risk of encryption algorithm and leakage of encryption	②-2	When electronic certificates are used for electronic signatures, network connections, etc., electronic certificates must be issued by trusted organizations.	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Google uses certificates and ACLs to achieve authentication integrity.	· ISO 27001 2013, Annex A.9
361	3.Technical measures	3.13. Use of encryption and electronic signature	②Managing encryption key and electronic signature to prevent the risk of encryption algorithm and leakage of encryption	②-3	In preparation for compromise of cryptographic algorithms and cryptographic keys, care should be taken to enable switching of cryptographic algorithms.	Google is certified to the ISO27001 Standard, which regulates "Cryptography" (ISO 27001:2013, Annex A.10) Customer data that is uploaded or created is encrypted at rest. We use several layers of encryption to protect customer data; adding redundant data protection and allowing us to select the optimal approach based on application requirements. Google publishes details about encryption and key management options for its Google Cloud Platform and Google Workspace products. To read more about key management and encryption, please see: https://cloud.google.com/security/encryption-at-rest/ https://services.google.com/fh/files/misc/google-workspace-encryption-wp.pdf Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including development of appropriate encryption measures.	· ISO 27001 2013, Annex A.10

362	3.Technical measures	3.13. Use of encryption and electronic signature	②Managing encryption key and electronic signature to prevent the risk of encryption algorithm and leakage of encryption	②-4	The public key certificate of the root certification authority for verifying data received from medical institutions should be obtained through a secure route and compared with fingerprints obtained through another route to verify the authenticity.	Not applicable. This is the customer's responsibility to respond to.	-
363	3.Technical measures	3.13. Use of encryption and electronic signature	②Managing encryption key and electronic signature to prevent the risk of encryption algorithm and leakage of encryption	②-5	When the cryptographic module uses an external source code or library, it is preferable to use the authenticity of the source code or library after verifying the integrity by electronic signatures or the like from the manufacturer.	Not applicable. This is the customer's responsibility to respond to.	-
364	3.Technical measures	3.13. Use of encryption and electronic signature	②Managing encryption key and electronic signature to prevent the risk of encryption algorithm	②-6	Cryptographic key generation is preferably implemented in secure environments such as tamper-resistant smart cards, USB tokens devices, etc.	Google is certified to the ISO27001 Standard, which regulates "Cryptography" (ISO 27001:2013, Annex A.10) Google publishes details about encryption and key management options for its Google Cloud Platform and Google Workspace products. To read more about key management and encryption, please see: https://cloud.google.com/security/encryption-in-transit/ https://services.google.com/fh/files/misc/google-workspace-encryption-wp.pdf	· ISO 27001 2013, Annex A.10

			and leakage of encryption			Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including development of appropriate encryption measures.	
365	3.Technical measures	3.13. Use of encryption and electronic signature	②Managing encryption key and electronic signature to prevent the risk of encryption algorithm and leakage of encryption	②-7	When key escrow is performed in preparation for loss of encryption keys, it is desirable to perform access control so that only legitimate management persons and legitimate processes can access the repositories of encryption keys.	Google is certified to the ISO27001 Standard, which regulates "Cryptography" (ISO 27001:2013, Annex A.10) Google publishes details about encryption and key management options for its Google Cloud and Google Workspace products. To read more about key management and encryption, please see: https://cloud.google.com/security/encryption-at-rest/ https://services.google.com/fh/files/misc/google-workspace-encryption-wp.pdf Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing cryptographic key management processes.	· ISO 27001 2013, Annex A.10
366	3.Technical measures	3.13. Use of encryption and electronic signature	②Managing encryption key and electronic signature to prevent the risk of encryption algorithm and leakage of encryption	②-8	In an environment in which an electronic signature applied to a document by a healthcare worker is verified based on an electronic signature method, it is desirable that signature verification can be continued without being affected by the weakening of a cryptographic algorithm.	Not applicable. This is the customer’s responsibility to respond to.	-
367	3.Technical measures	3.14. Access management of remote	①Access management to prevent unnecess	①-1	When maintenance is performed by remote maintenance, appropriate safety grip actions such as setting up access points, restricting protocols, and access authority grip should be taken as needed.	Google is certified to the ISO27001 Standard, which regulates "Supplier Relationships" (ISO 27001:2013, Annex A.15). Information security oversight and management controls, including vendor security practices are reviewed and verified by a third party auditor for Google's SOC 2, Type II report.	· ISO 27001 2013, Annex A.15

		maintenance	ary login of remote maintenance			Google directly conducts virtually all data processing activities to provide our services. However, Google may engage some third-party suppliers to provide services related to Cloud Platform, including customer and technical support. Prior to onboarding third-party suppliers, Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms.	
368	3.Technical measures	3.15. Management for Electronic signature	①Use of Electronic Certificates Issued by a Trusted Third Party Organization	①-1	When using an electronic signature in the medical information systems, use a digital certificate issued by trusted third party organization, such as an electronic certificate for signature, issued by the PKI authentication center in the field of health, medical and welfare.	Not applicable. This is the customer's responsibility to respond to.	-
369	3.Technical measures	3.15. Management for Electronic signature	②Timestamping when applying Electronic signature	②-1	Agree with medical institutions about contents and verification methods, when time stamping to information, contains electronic signature.	Not applicable. This is the customer's responsibility to respond to..	-
370	3.Technical measures	3.15. Management for Electronic signature	②Timestamping when applying Electronic signature	②-2	When dealing with time-stamped information, agree with medical institutions on verifying and responding to the validity of the time-stamp within the legal retention period.	Not applicable. This is the customer's responsibility to respond to.	-
371	3.Technical measures	3.15. Management for Electronic signature	②Timestamping when applying Electronic signature	②-3	Agree with medical institutions, in case of preserving time stamped information for long term period.	Not applicable. This is the customer's responsibility to respond to.	-
372	3.Technical measures	3.15. Management for Electronic signature	③Using valid electronic certificates at the point of	③-1	When dealing with time-stamped information, agree with medical institutions on the method of time stamping to ensure the validity of electronic signatures before invalidation of digital certificates.	Not applicable. This is the customer's responsibility to respond to.	-

			timestamping				
373	3.Technical measures	3.16. Installation of Tampering prevention and detection	①Implementation of software for preventing alternation and detection measures	①-1	Perform software integrity checking (tampering detection) periodically to verify that tampering has not been made.	Google is certified to the ISO27001 Standard, which regulates "Logging and Monitoring" (ISO 27001:2013, Annex A.12.4). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's security monitoring program is focused on information gathered from internal network traffic, employee actions on systems and outside knowledge of vulnerabilities. At many points across our global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. This analysis is performed using a combination of open-source and commercial tools for traffic capture and parsing. A proprietary correlation system built on top of Google technology also supports this analysis. Network analysis is supplemented by examining system logs to identify unusual behavior, such as attempted access of customer data. Google security engineers place standing search alerts on public data repositories to look for security incidents that might affect the company's infrastructure. They actively review inbound security reports and monitor public mailing lists, blog posts, and wikis. Automated network analysis helps determine when an unknown threat may exist and escalates to Google security staff, and network analysis is supplemented by automated analysis of system logs. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuration of specific monitoring to detect false or unverified data.	· ISO 27001 2013, Annex A.12.4
374	3.Technical measures	3.16. Installation of Tampering prevention and detection	①Implementation of software for preventing alternation and detection measures	①-2	In order to avoid the risk of unauthorized software rewriting, tampering prevention and detection measures should be implemented on the software when the developed software is introduced into the operation facility.	Google is certified to the ISO27001 Standard, which regulates "Change Management" (ISO27001:2013 Annex A 12.1.2) and "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14). Please see the Google Infrastructure Security Design Overview - https://cloud.google.com/security/security-design/ for more details. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including change management and system development procedures.	· ISO 27001 2013, Annex A.12.1.2,14
375	3.Technical measures	3.17. Management of data for each patient	①Implementing Information management function for individual patient	①-1	Services include the ability to grip medical-of-care informations on a patient-by-patient basis.	Not applicable. This is the customer's responsibility to respond to.	-

376	3.Technical measures	3.18. Ensuring response time based on purpose	①Ensuring response time based on the purpose of using medical information system	①-1	Agree with medical institutions on response time (general display speed, display time of search results) when medical institutions use medical information systems.	Not applicable. This is the customer's responsibility to respond to.	-
377	3.Technical measures	3.19. Incident measures by Redundancy	①Redundancy in case of medical information system outage	①-1	Implement measures such as preparing substitute equipment, making it redundant, and installing backup facilities so that work can be continued even in the event of a failure of an information processing apparatus.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	· ISO 27001 2013, Annex A.17.2
378	3.Technical measures	3.19. Incident measures by Redundancy	①Redundancy in case of medical information system outage	①-2	Concerning the medical information system and the network, measures for redundancy are necessary for continuing services, not to affect normal medical treatments.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural	· ISO 27001 2013, Annex A.17.1

						disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	
379	3.Technical measures	3.19. Incident measures by Redundancy	①Redundancy in case of medical information system outage	①-3	Agree with medical institutions based on ①-2, to ensure the quality of continuity of the service in the event of failures.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	· ISO 27001 2013, Annex A.17.1
380	3.Technical measures	3.19. Incident measures by Redundancy	①Redundancy in case of medical information system outage	①-4	Agree with medical institutions on alternative measures to ensure continuity in the event of failures.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services	· ISO 27001 2013, Annex A.17.1

						themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	
381	3.Technical measures	3.19. Incident measures by Redundancy	②Disk Failure Protection	②-1	When storing information of the medical records in a recording device such as hard disk, countermeasures against disk failures equivalent to RAID-1 or RAID-6 or more should be taken.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	· ISO 27001 2013, Annex A.17.1
382	3.Technical measures	3.20. Measures for	①Implementation of function in	①-1	When storing medical information in medical institutions, agree with medical institutions to provide information on measures that can be taken by medical	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2), and "Backup" (ISO27001:2013 Annex A 12.3.), and "Documented Operating Procedures" (ISO27001:2013, Annex A 12.1.1). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report.	· ISO 27001 2013, Annex A.17.2,12.3,12.1.1.

		system incident	case of medical information system failure		institutions to ensure readability in the event of a failure.	Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	
383	3.Technical measures	3.20. Measures for system incident	①Implementation of function in case of medical information system failure	①-2	Assess the magnitude of the impact of hardware and software, and consider measures such as making the system part redundant, or allowing the system part to be outputted to external files in a format that ensures readability (format such as PDF, JPEG, or PNG) so that information can be browsed using general-purpose browsers, etc. in case the system becomes unable to be browsed due to a disability.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	· ISO 27001 2013, Annex A.17.1

Guidelines for Safety Management of Medical Information by Providers of Information Systems and Services Handling Medical Information

Handbook for Google Cloud and Google Workspace

384	3.Technical measures	3.20. Measures for system incident	①Implementation of function in case of medical information system failure	①-3	When storing medical information in medical institutions, agree with medical institutions on the availability and content of functions related to the output of external files required to ensure readability in the event of a failure.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2), and "Backup" (ISO27001:2013 Annex A 12.3.), and "Documented Operating Procedures" (ISO27001:2013, Annex A 12.1.1). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	· ISO 27001 2013, Annex A.17.2,12.3,12.1.1.
385	3.Technical measures	3.20. Measures for system incident	①Implementation of function in case of medical information system failure	①-4	In the case of storing medical information is stored in medical institutions, agree with medical institution on the usage of functions, provisioning information, conditions for backup data stored in remote locations to ensure readability in the event of a failure.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions.	· ISO 27001 2013, Annex A.17.2

386	3.Technical measures	3.20. Measures for system incident	①Implementation of function in case of medical information system failure	①-5	Agree on the inclusion of functions (e.g. screen printing functions, file downloading functions, etc.) in the service to support the assurance of readability of medical records at medical institutions in case of emergency, and the provision of information such as security needed for the service.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2), and "Backup" (ISO27001:2013 Annex A 12.3.), and "Documented Operating Procedures" (ISO27001:2013, Annex A 12.1.1). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	· ISO 27001 2013, Annex A.17.2,12.3,12.1.1.
387	3.Technical measures	3.20. Measures for system incident	①Implementation of function in case of medical information system failure	①-6	After clarifying the division of the role in case of failure, agree with medical institutions on the scope of services to ensure operation.	Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Google Cloud Terms of Service: https://cloud.google.com/terms/ Google Workspace Terms of Use: https://workspace.google.com/terms/dpa_terms.html SLA: https://cloud.google.com/terms/sla/ https://workspace.google.com/terms/sla.html	-
388	3.Technical measures	3.21. Management of backup and restoration	①Management of backup and restoration	①-1	Storage in a storage environment specified by the manufacturer of the media to minimize the risk of loss of information due to damage to electronic media, etc.	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001:2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A.11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure	· ISO 27001 2013, Annex A.8.1,8.3.2,11.2.7,12.5

						the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	
389	3.Technical measures	3.21. Management of backup and restoration	①Management of backup and restoration	①-2	Actions should be taken to provide the remaining amount of storable resources that can be used by each medical institution at any time.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support data file management activities.	· ISO 27001 2013, Annex A.17.2,12.3
390	3.Technical measures	3.21. Management of backup and restoration	①Management of backup and restoration	①-3	When medical institutions use the medical information systems, agree with medical institutions on information on available resources (storage capacity, usable period, risk, backup frequency, backup method, etc.) .	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is	· ISO 27001 2013, Annex A.17.2,12.3

						automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support data file management activities.	
391	3.Technical measures	3.21. Management of backup and restoration	①Management of backup and restoration	①-4	Include the location (internal, portable medium) where the medical information system stores information, the storage capacity, the storage period, and the risk for each location in the operational management regulations.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support data file management activities.	· ISO 27001 2013, Annex A.17.2,12.3
392	3.Technical measures	3.21. Management of backup and restoration	①Management of backup and restoration	①-5	In the case of using the medical information system provided by another provider described in ①-4, similar information is collected and handled. When using a medical information systems on a virtualization technology, the contractor checks information about resources that can be used under contract with other operators.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a	· ISO 27001 2013, Annex A.17.2,12.3

						solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support data file management activities.	
393	3.Technical measures	3.21. Management of backup and restoration	①Management of backup and restoration	①-6	Education about management method regulated by Operation Management Regulations will be provided to employees, due to ①-4.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support data file management activities.	· ISO 27001 2013, Annex A.17.2,12.3
394	3.Technical measures	3.21. Management of backup and	①Management of backup and	①-7	The subcontractor related to medical information systems shall be requested to respond to the management methods specified in ①-4 of Operation Management Regulations.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report.	· ISO 27001 2013, Annex A.17.2,12.3

		restoration	restoration			Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support data file management activities.	
395	3.Technical measures	3.21. Management of backup and restoration	①Management of backup and restoration	①-8	In cases where information is damaged, actions are taken to recover quickly, and the details and procedures should be included in the Operation grip Rules, etc.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support data file management activities.	· ISO 27001 2013, Annex A.17.2,12.3
396	3.Technical measures	3.21. Manage	①Management of	①-9	Include in the Operation Management Regulations, measures to be taken in the event that the recovery of	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and	· ISO 27001 2013, Annex A.17.2,12.3

		ment of backup and restoration	backup and restoration		damaged information becomes difficult due to the measures shown in ①-8.	integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support data file management activities.	
397	3.Technical measures	3.21. Management of backup and restoration	①Management of backup and restoration	①-10	Agree with medical institutions about the scope of responsibility and exemption conditions for the damaged information.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions.	· ISO 27001 2013, Annex A.17.2,12.3

						Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support data file management activities.	
398	3.Technical measures	3.21. Management of backup and restoration	①Management of backup and restoration	①-11	Obtain backups of the medical information system based on the results of the risk analysis. Determine the object, frequency, storage method/medium, management method of obtained backups and include the details in the operation management regulations.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support data file management activities.	· ISO 27001 2013, Annex A.17.2,12.3
399	3.Technical measures	3.21. Management of backup and restoration	①Management of backup and restoration	①-12	Regarding the backups acquired, necessary periodic inspection is performed in accordance with the management method of the recording medium to confirm that the recording contents are not altered or destroyed.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously	· ISO 27001 2013, Annex A.17.2,12.3

						replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support data file management activities.	
400	3.Technical measures	3.21. Management of backup and restoration	②Management of recording medium for backup	②-1	For the backup to be stored in the recording medium, the backup content, the use starting date, and the use ending date are clarified based on the characteristics of the medium (tape/disk, capacity, etc.), and the grip is made.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support data file management activities.	· ISO 27001 2013, Annex A.17.2,12.3
401	3.Technical measures	3.21. Management of backup and restoration	②Management of recording medium for backup	②-2	When the end date of use of the backup recording medium as the target is approaching, the contents thereof are copied to another medium or the like before the end date.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption.	· ISO 27001 2013, Annex A.17.2,12.3

						Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support data file management activities.	
402	3.Technical measures	3.21. Management of backup and restoration	②Management of recording medium for backup	②-3	Copy the electronic media to other media when the effective use limit period of the electronic media approaches so that the effective use limit period specified by the manufacturer is not exceeded.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support data file management activities.	· ISO 27001 2013, Annex A.17.2,12.3
403	3.Technical measures	3.21. Management of backup and restoration	②Management of recording medium for backup	②-4	Including the procedure of ②-1 to ②-3 in the operation management regulations, will provide necessary education to employees and subcontractors.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is	· ISO 27001 2013, Annex A.17.2,12.3

						automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support data file management activities.	
404	3.Technical measures	3.21. Management of backup and restoration	②Management of recording medium for backup	②-5	Agree with medical institutions to provide backup-related information.	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud Platform and Google Workspace customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing a process to support data file management activities.	· ISO 27001 2013, Annex A.17.2,12.3
405	3.Technical measures	3.22. Ensuring compatibility for system change and	①Ensuring compatibility of data format and protocol	①-1	For data items such as medical records, the standards for the field of health and medical information in the MHLW (hereinafter referred to as "MHLW standards") shall be adopted.	Not applicable. This is the customer's responsibility to respond to.	-

		improvement					
406	3.Technical measures	3.22. Ensuring compatibility for system change and improvement	①Ensuring compatibility of data format and protocol	①-2	Regarding data items for which the standard of the Ministry of Health, Labour and Welfare is not established, the data format shall be easy to convert and agreed with medical institutions.	Not applicable. This is the customer's responsibility to respond to.	-
407	3.Technical measures	3.22. Ensuring compatibility for system change and improvement	①Ensuring compatibility of data format and protocol	①-3	The information systems are provided with functions and validation methods that prevent changes in information in medical records, such as record grip methods and actions to be taken when changing the master table of medical information.	Not applicable. This is the customer's responsibility to respond to.	-
408	3.Technical measures	3.22. Ensuring compatibility for system change and improvement	①Ensuring compatibility of data format and protocol	①-4	Agree with medical institutions, etc. on the procedures for updating and migrating information systems when it is difficult to provide the functions shown in ①-3.	Not applicable. This is the customer's responsibility to respond to.	-
409	3.Technical measures	3.22. Ensuring compatibility for system change and improvement	①Ensuring compatibility of data format and protocol	①-5	Support the use of previous data formats and protocols for storing and exchanging medical information, if the protocol changes, while the pre-change data formats, medical institutions using the protocol, etc. exist.	Google is certified to the ISO27001 Standards, which regulates "Operational Procedures and Responsibilities" (ISO 27001:2013, Annex A.12.1) and "Network Security" (ISO 27001:2013, Annex A.13.1). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. System changes that may affect security, availability, processing integrity, or confidentiality are communicated to management and users who will be affected.	· ISO 27001 2013, Annex A.12.1
410	3.Technical measures	3.22. Ensuring compatibility for	①Ensuring compatibility of data	①-6	When attempting to upgrade or change the data format or transfer protocol, confirm the impact on the use of the service.	Google is certified to the ISO27001 Standards, which regulates "Operational Procedures and Responsibilities" (ISO 27001:2013, Annex A.12.1) and "Network Security" (ISO 27001:2013, Annex A.13.1).	· ISO 27001 2013, Annex A.12.1

		system change and improvement	format and protocol			Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. System changes that may affect security, availability, processing integrity, or confidentiality are communicated to management and users who will be affected.	
411	3.Technical measures	3.22. Ensuring compatibility for system change and improvement	①Ensuring compatibility of data format and protocol	①-7	As a result of ①-6, if it is deemed that the use of the service is affected, the medical institution will notify of the version upgrade or change in anticipation of a sufficient period of time to respond, and provide specific information on the measures necessary for the response.	Google is certified to the ISO27001 Standards, which regulates "Operational Procedures and Responsibilities" (ISO 27001:2013, Annex A.12.1) and "Network Security" (ISO 27001:2013, Annex A.13.1). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. System changes that may affect security, availability, processing integrity, or confidentiality are communicated to management and users who will be affected.	· ISO 27001 2013, Annex A.12.1
412	3.Technical measures	3.22. Ensuring compatibility for system change and improvement	①Ensuring compatibility of data format and protocol	①-8	①-7 shall be conducted in consideration of data linkage with other medical information systems. Agreement with medical institutions on the provision of information regarding ensuring compatibility with medical institutions.	Google is certified to the ISO27001 Standards, which regulates "Operational Procedures and Responsibilities" (ISO 27001:2013, Annex A.12.1) and "Network Security" (ISO 27001:2013, Annex A.13.1). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. System changes that may affect security, availability, processing integrity, or confidentiality are communicated to management and users who will be affected.	· ISO 27001 2013, Annex A.12.1
413	3.Technical measures	3.22. Ensuring compatibility for system change and improvement	①Ensuring compatibility of data format and protocol	①-9	As a result of the change of the data format/transfer protocol, when the medical institution or the like terminates the use of the service, measures are taken to ensure readability.	Google is certified to the ISO27001 Standards, which regulates "Operational Procedures and Responsibilities" (ISO 27001:2013, Annex A.12.1) and "Network Security" (ISO 27001:2013, Annex A.13.1). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. System changes that may affect security, availability, processing integrity, or confidentiality are communicated to management and users who will be affected.	· ISO 27001 2013, Annex A.12.1
414	3.Technical measures	3.22. Ensuring compatibility for system change and improvement	①Ensuring compatibility of data format and protocol	①-10	With regard to devices and software related to medical information systems, the decision will be made with a view to ensuring compatibility in the future, and the risk of changes in standard specifications, will also be considered.	Google is certified to the ISO27001 Standards, which regulates "Operational Procedures and Responsibilities" (ISO 27001:2013, Annex A.12.1) and "Network Security" (ISO 27001:2013, Annex A.13.1). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. System changes that may affect security, availability, processing integrity, or confidentiality are communicated to management and users who will be affected.	· ISO 27001 2013, Annex A.12.1

415	3.Technical measures	3.22. Ensuring compatibility for system change and improvement	①Ensuring compatibility of data format and protocol	①-11	When a service is provided using medical information systems provided by another service providers, measures are taken to prevent a problem from occurring in the contractors' service provision even when another providers stop the services. In case some or all of the services provided by another providers are stopped or changed (minor version upgrades are not included) due to the stoppage or change of the service of another providers, take countermeasures of preventing equipments from deterioration.	Google is certified to the ISO27001 Standards, which regulates "Operational Procedures and Responsibilities" (ISO 27001:2013, Annex A.12.1) and "Network Security" (ISO 27001:2013, Annex A.13.1). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. System changes that may affect security, availability, processing integrity, or confidentiality are communicated to management and users who will be affected.	· ISO 27001 2013, Annex A.12.1
416	3.Technical measures	3.22. Ensuring compatibility for system change and improvement	①Ensuring compatibility of data format and protocol	①-12	When updating the equipment or software related to the medical information system, or changing the service provided by another service providers, consider ①-10 and ①-11.	Google is certified to the ISO27001 Standards, which regulates "Operational Procedures and Responsibilities" (ISO 27001:2013, Annex A.12.1) and "Network Security" (ISO 27001:2013, Annex A.13.1). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. System changes that may affect security, availability, processing integrity, or confidentiality are communicated to management and users who will be affected.	· ISO 27001 2013, Annex A.12.1