Annual Report to Congress on Breaches of Unsecured Protected Health Information

For Calendar Year 2019

As Required by the
Health Information Technology for Economic and Clinical Health (HITECH) Act,
Public Law 111-5, Section 13402

Submitted to the
Senate Committee on Finance,
Senate Committee on Health, Education, Labor, and Pensions,
House Committee on Ways and Means, and
House Committee on Energy and Commerce

U.S. Department of Health and Human Services
Office for Civil Rights

Introduction

Section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5), requires covered entities and business associates under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to provide notification of breaches of unsecured protected health information (PHI).

Section 13402(i) of the HITECH Act requires the Secretary of Health and Human Services ("the Secretary") to prepare and submit to the Senate Committee on Finance, the Senate Committee on Health, Education, Labor, and Pensions, the House Committee on Ways and Means, and the House Committee on Energy and Commerce an annual report containing:

- The number and nature of breaches reported to the Secretary, and
- The actions taken in response to those breaches.

The following report provides the required information for the breaches reported to the Secretary that occurred in calendar year 2019.[1]

Background

Section 13402 of the HITECH Act requires HIPAA covered entities to notify affected individuals, the Secretary, and in some cases, the media, following the discovery of a breach of unsecured PHI. Business associates are required to notify covered entities following the discovery of a breach of unsecured PHI. Section 13402(h) of the HITECH Act defines "unsecured protected health information" as "protected health information that is not secured through the use of a technology or methodology specified by the Secretary in guidance" and mandates that the Secretary issue guidance specifying the technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized persons. The guidance issued by the Secretary identifies encryption and destruction processes as tested by the National Institute of Standards and Technology as the two technologies and methodologies for rendering PHI unusable, unreadable, or indecipherable to unauthorized persons.[2] Covered entities and business associates that encrypt or destroy PHI in accordance with the guidance are not required to provide notifications in the event of a breach of such information because such information is not considered "unsecured."

The U.S. Department of Health & Human Services ("the Department") issued its Breach Notification for Unsecured Protected Health Information Interim Final Rule (74 FR 42740) on August 24, 2009, to implement the breach notification requirements of section 13402 of the HITECH Act with respect to HIPAA covered entities and business associates. On January 25,

[1] All previous Reports to Congress are available on the Office for Civil Right's website: https://www.hhs.gov/hipaa/for-professionals/breach-notification/reports-congress/index.html
[2] https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html.

2013, the Department published modifications to and made permanent the provisions of the Breach Notification Rule (78 FR 5566).

The Office for Civil Rights (OCR) is the office within the Department that is responsible for administering and enforcing the HIPAA Privacy, Security, and Breach Notification Rules.

Definition of Breach

Consistent with the definition of breach in section 13400(1)(A) of the HITECH Act, the Department defines "breach" at 45 CFR § 164.402 as the "acquisition, access, use, or disclosure of PHI in a manner not permitted by [the HIPAA Privacy Rule[3]] which compromises the security or privacy of the PHI." Under the Breach Notification Rule, unauthorized acquisition, access, use, or disclosure of PHI (that does not fall into one of the enumerated exceptions discussed below) is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment. This risk assessment must address at least the following factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person(s) who used the PHI or to whom the disclosure was made;
3. Whether the PHI was actually acquired or viewed; and
4. The extent to which the risk to the PHI has been mitigated.[4]

Section 13400(1)(B) of the HITECH Act provides several exceptions to the definition of "breach." These exceptions are set forth in the regulations at 45 CFR § 164.402. Section 164.402 excludes as a breach: (1) any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or business associate, if made in good faith and within the scope of authority, and if it does not result in further impermissible use or disclosure; (2) any inadvertent disclosure of PHI by a person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received is not further impermissibly used or disclosed; and (3) a disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain the information.

Breach Notification Requirements

Following the discovery of a breach of unsecured PHI, covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain cases, the media. In the case

[3] The Privacy Rule strikes a balance that protects the privacy of the health information of individuals while permitting important uses and disclosures of the information, such as for treatment of an individual and payment for health care, for certain public health purposes, in emergency situations, and to the friends and family involved in the care of an individual.

[4] *See* 45 CFR § 164.402 (definition of "breach").

of a breach of unsecured PHI at or by a business associate of a covered entity, the business associate must notify the covered entity of the breach.[5] These breach notification requirements for covered entities and business associates are set forth at 45 CFR §§ 164.404 – 164.410.

- **Individual Notice**

Covered entities must notify affected individuals of a breach of unsecured PHI without unreasonable delay and no later than 60 calendar days following discovery of the breach. Covered entities must provide written notification by first-class mail at the last known address of the individual or, if the individual agrees to electronic notice, by e-mail. If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual, then the covered entity must provide written notification to the next of kin or personal representative. Individual notification may be provided in one or more mailings as information becomes available regarding the breach.

If the covered entity has insufficient or out-of-date contact information for 10 or more individuals, the covered entity must provide substitute notice in the form of either a conspicuous posting for 90 days on the home page of its Web site or conspicuous notice in major print or broadcast media in geographic areas where the affected individuals likely reside, and include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's information may be included in the breach. In cases in which the covered entity has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written notice, telephone, or other means.

Whatever the method of delivery, the notification must include, to the extent possible: (1) a brief description of what happened, including the date of the breach and the date of discovery of the breach, if known; (2) a description of the types of unsecured PHI involved in the breach; (3) any steps individuals should take to protect themselves from potential harm resulting from the breach; (4) a brief description of what the covered entity is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and (5) contact information for individuals to ask questions or learn additional information.[6]

- **Media Notice**

For breaches involving more than 500 residents of a State or jurisdiction, a covered entity must notify prominent media outlets serving the State or jurisdiction. Like individual notice, this media notification must be provided without unreasonable delay and no later than 60 calendar days

[5] The Breach Notification Rule requires business associates to report to the covered entity the breach of unsecured PHI within 60 days of discovery. Through the business associate agreement, the parties may add additional specificity regarding the breach notification obligations of the business associate, such as a stricter timeframe for the business associate to report a potential breach to the covered entity and/or whether the business associate will handle breach notifications to individuals, HHS, and the media, as applicable, on behalf of the covered entity.
[6] *See* 45 CFR § 164.404.

following the discovery of a breach. It must include the same information as that required for the individual notice.[7]

- **Notice to the Secretary**

In addition to notifying affected individuals and the media (where appropriate), a covered entity must notify the Secretary of breaches of unsecured PHI. If a breach involves 500 or more individuals, a covered entity must notify the Secretary at the same time the affected individuals are notified of the breach. 45 CFR § 164.408(b). If a breach involves fewer than 500 individuals, covered entities may submit reports of such breaches on an annual basis. Reports of breaches involving fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches were discovered.[8] Covered entities must notify the Secretary by filling out and electronically submitting a breach report form on the Department website at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.

- **Notification by a Business Associate**

If a breach of unsecured PHI occurs at or by a business associate, the business associate must notify the covered entity following the discovery of the breach. A business associate must provide notice to the covered entity without unreasonable delay and no later than 60 calendar days from the discovery of the breach (although a covered entity and business associate may negotiate stricter timeframes for the business associate to report a breach to the covered entity). To the extent possible, the business associate's report to the covered entity must identify each individual affected by the breach, as well as include any other available information that is required to be included in the notification to individuals. While a covered entity ultimately maintains the obligation to notify the affected individuals, the Secretary, and the media (if appropriate) where a breach occurs at or by its business associate, a covered entity may, pursuant to agreement with its business associate(s), delegate the responsibility of providing the required notifications to the business associate that suffered the breach or to another of its business associates.[9]

Summary of Breach Reports

This report describes the types and numbers of breaches reported to OCR that occurred between January 1, 2019, and December 31, 2019, and describes actions that have been taken by covered entities and business associates in response to these breaches.

This report generally describes OCR investigations and enforcement actions with respect to the reported breaches. Additional information on OCR's compliance and enforcement efforts in

[7] *See* 45 CFR § 164.406.
[8] *See* 45 CFR § 164.408(c).
[9] *See* Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the HITECH Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 FR 5566, 5656 (January 25, 2013). *See* 45 CFR § 164.410.

other areas may be found in OCR's Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance for the Calendar Year of 2019. OCR opens compliance reviews to investigate all reported breaches affecting 500 or more individuals, and may open compliance reviews into reported breaches affecting fewer than 500 individuals. As discussed in greater detail below, in addition to requiring covered entities and business associates to take corrective action in hundreds of cases, for 2019, OCR resolved five breach investigations with resolution agreements/corrective action plans or imposed civil money penalties totaling more than $6.9 million in collections.

Breaches Involving 500 or More Individuals

Notification to the Secretary of breaches involving 500 or more individuals must occur contemporaneously with notice to affected individuals. OCR received 408 reports of such breaches for calendar year 2019,[10] which affected a total of approximately 38,732,966 individuals.[11]

Breaches in 2019 Affecting 500 or More Individuals[12]

For the 408 breaches affecting 500 or more individuals in 2019, OCR received:

(1) 327 reports (80%) of breaches from health care providers (affecting 21,915,146 individuals (57%));
(2) 39 reports (10%) of breaches from health plans (affecting 3,278,850 individuals (8%));
(3) 40 reports (10%) of breaches from business associates (affecting 11,972,032 individuals (31%)); and
(4) 2 reports (<1%) of breaches from health care clearinghouses (affecting 1,566,938 individuals (4%)).

See Figures 1 and 2.

[10]The Department receives some reports where the breach occurred over a period of several years. For the purposes of this report, breach incidents spanning multiple years are included with the data for the last year in which the breach occurred (*e.g.*, a breach incident that continued from 2017 into 2019 would be reported with the 2019 figures).
[11] The numbers of affected individuals provided throughout this report are approximate because some covered entities reported uncertainty about the number of records affected by a breach.
[12] Throughout this report, in instances in which the percentage is less than one, the percentage is not reported.

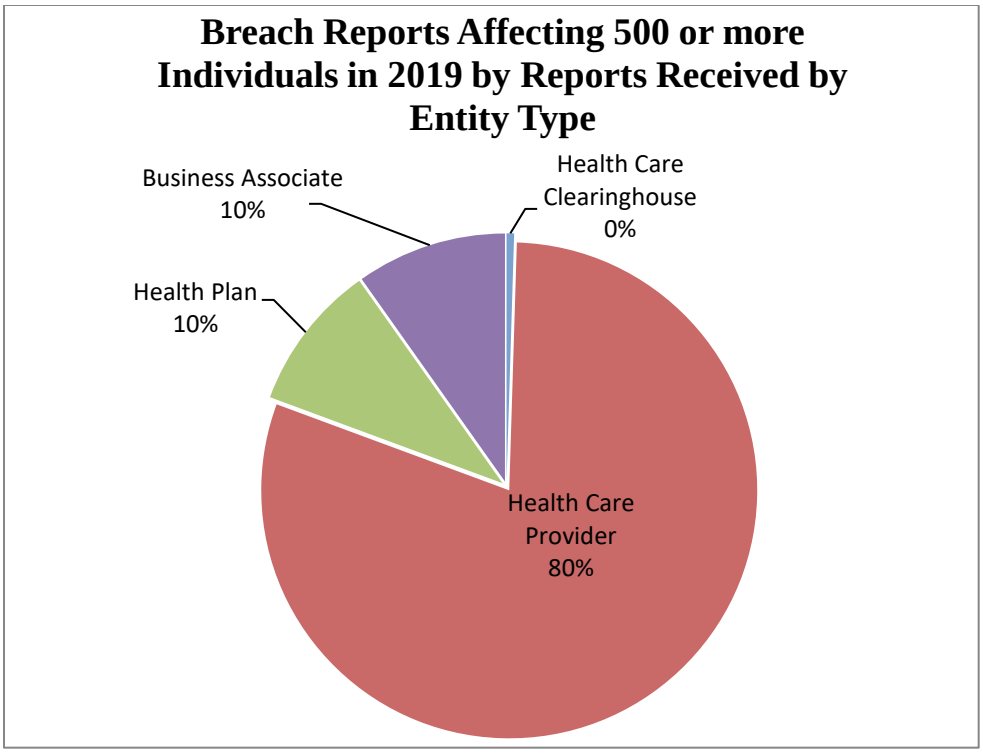

Figure 1

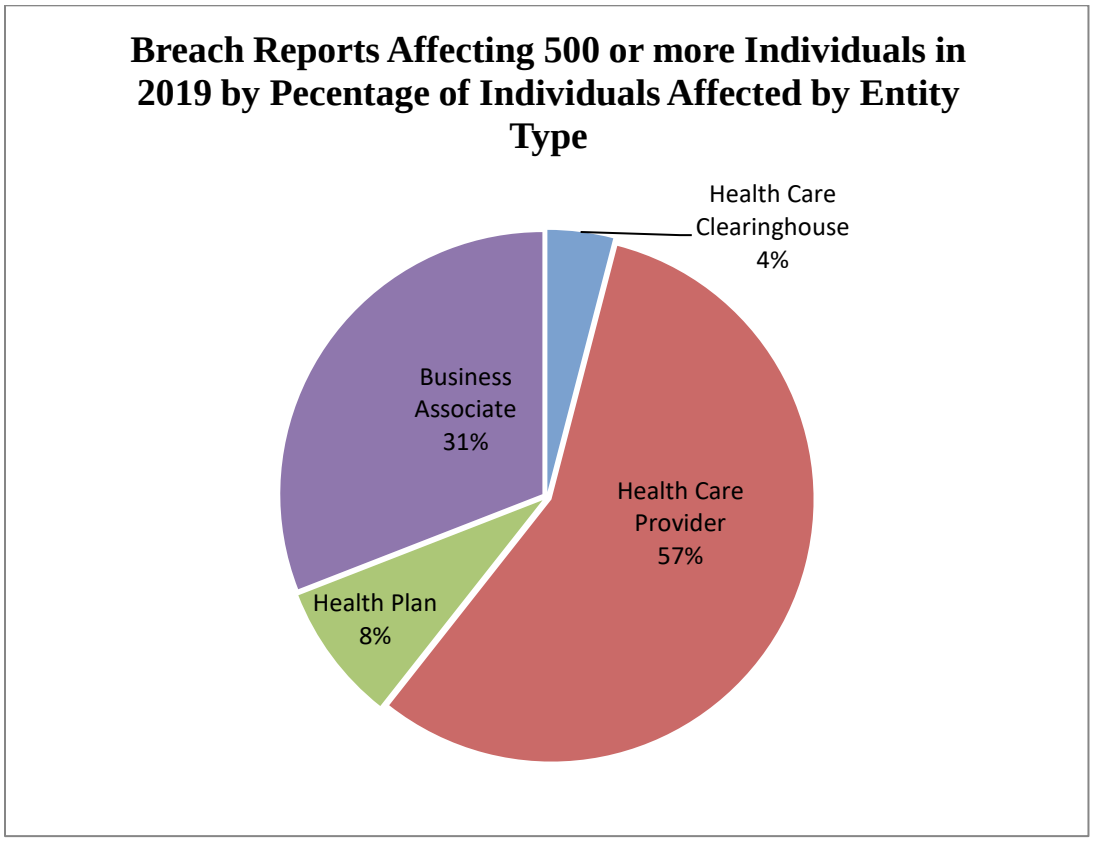

Figure 2

The 408 reports submitted to OCR for breaches affecting 500 or more individuals occurring in 2019 can be categorized by five general causes as follows (in order of frequency):

(1) Hacking/IT incident of electronic equipment or a network server (234 reports (57%) affecting 33,936,326 individuals (88%));
(2) Unauthorized access or disclosure of records containing PHI (125 reports (31%) affecting 4,466,465 individuals (12%));
(3) Theft of electronic equipment/portable devices or paper containing PHI (29 reports (7%) affecting 232,257 individuals (1%));
(4) Loss of electronic media or paper records containing PHI (15 reports (4%) affecting 73,637 individuals (<1%)); and
(5) Improper disposal of PHI (5 reports (1%) affecting 24,281 individuals (<1%)).

See Figures 3 and 4.

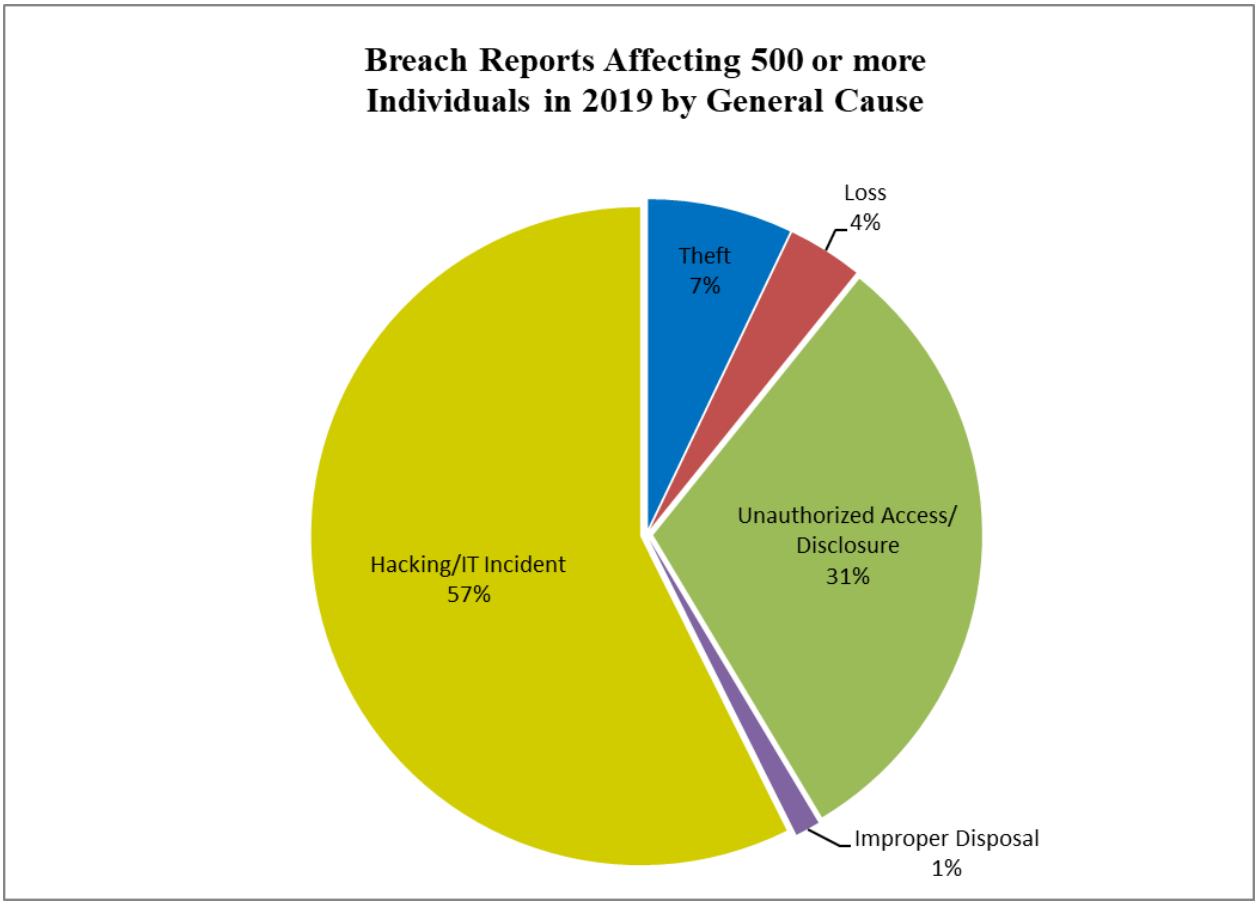

Figure 3

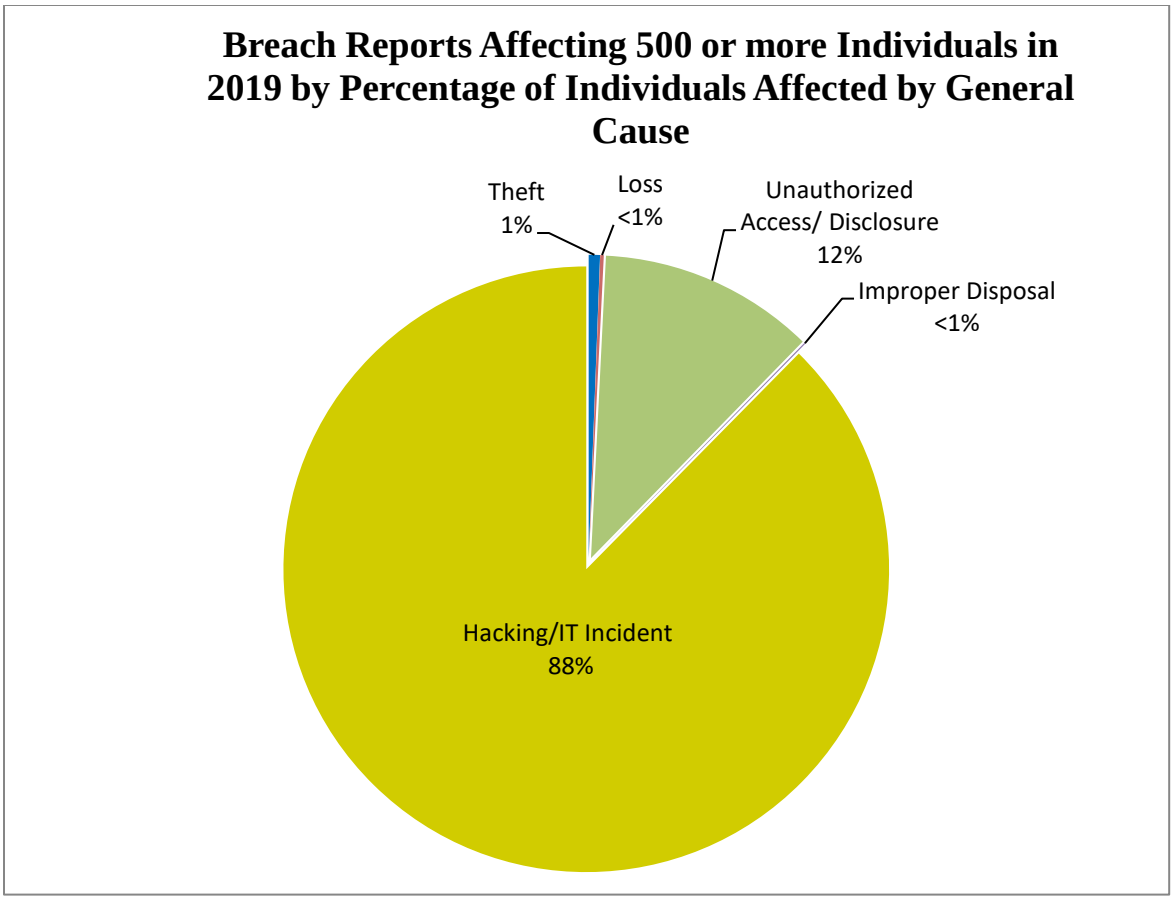
Breach Reports Affecting 500 or more Individuals in 2019 by Percentage of Individuals Affected by General Cause
Theft 1%
Loss <1%
Unauthorized Access/ Disclosure 12%
Improper Disposal <1%
Hacking/IT Incident 88%

Figure 4

The 408 reports submitted to OCR for breaches occurring in 2019 described the following locations of the PHI (in order of frequency):

(1) E-mail (160 reports (39%) affecting 2,037,226 individuals (5%));
(2) Network server (88 reports (22%), affecting 33,126,677 individuals (86%));
(3) Paper (43 reports (10%) affecting 129,218 individuals (<1%));
(4) Other (40 reports (10%) affecting 2,449,611 individuals (6%));[13]
(5) Desktop computer (27 reports (7%) affecting 434,688 individuals (1%));
(6) Electronic medical record (24 reports (6%), affecting 337,385 individuals (1%));
(7) Laptop computer (16 reports (4%), affecting 152,016 individuals (< 1%)); and
(8) Other portable electronic device (10 reports (2%), affecting 66,145 individuals (<1%)).

See Figures 5 and 6.

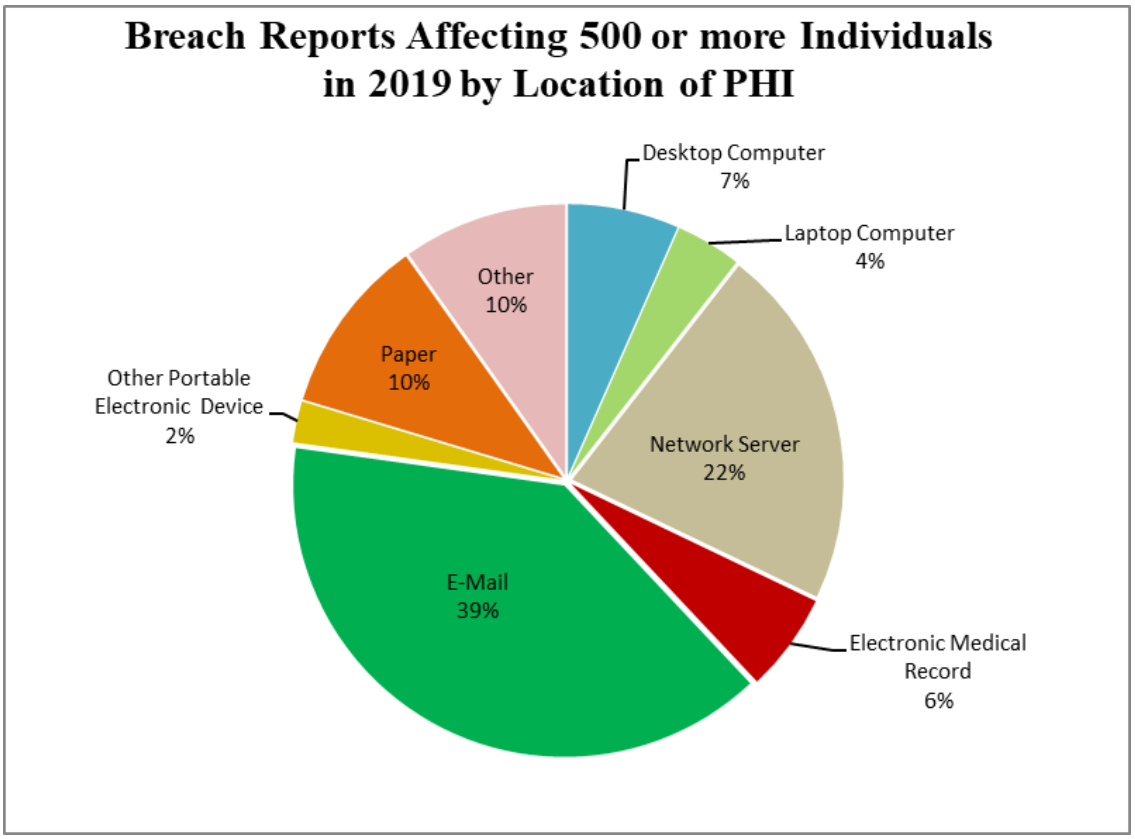

Figure 5

[13] Other is used when a covered entity is unable to identify the specific location of the breach, such as when an impersonator has accessed data, or data is taken by an employee, but the covered entity is not certain of the PHI's location when it was disclosed.

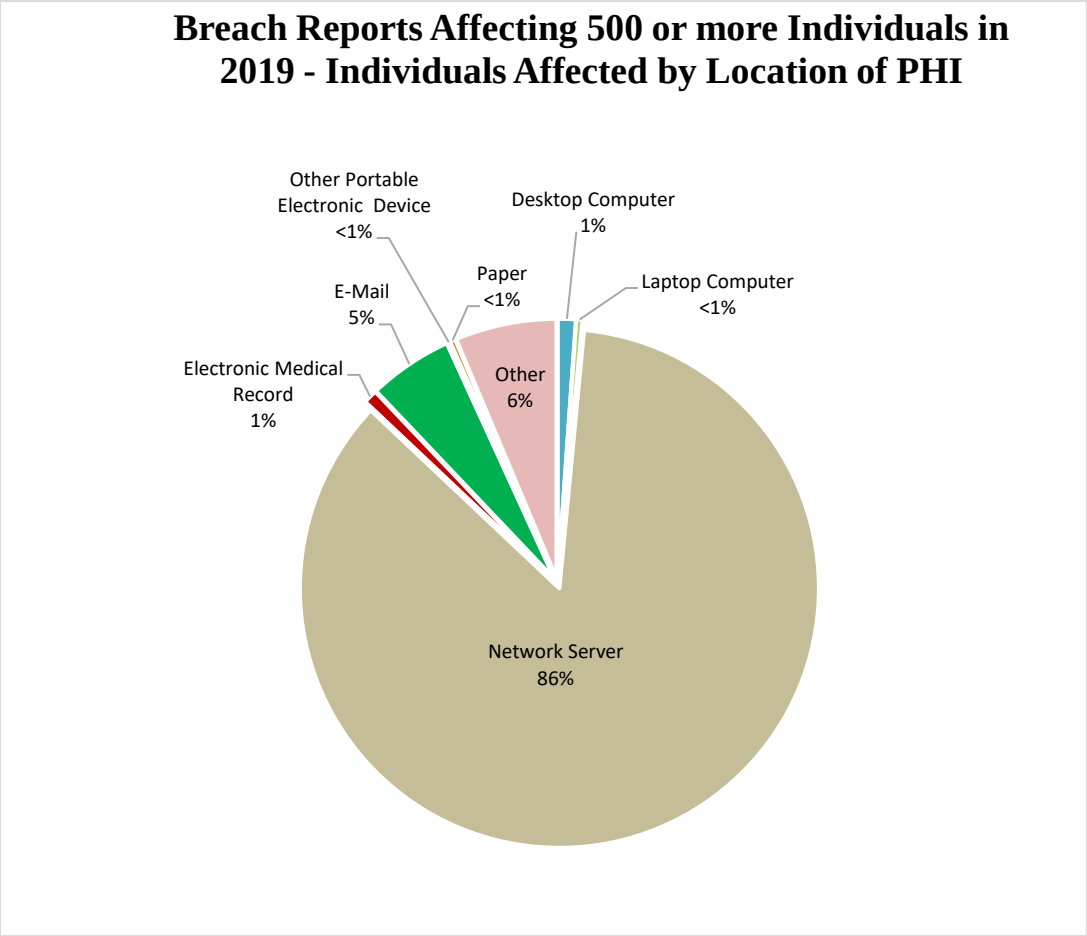

Figure 6

Largest breaches in 2019 for each reported cause

This section describes the largest breach, by number of individuals affected, for each of the five reported causes, followed by a short summary of scenarios reported for each cause.

Hacking/IT Incident of Electronic Equipment or Network Server: The largest breach in 2019 resulting from a hacking/IT incident involved a hacker who penetrated the server of a business associate containing PHI. The breach incident affected approximately 11,500,000 individuals. Other hacking/IT incidents involved the use of malware, ransomware, phishing (*e.g.*, employees opening email attachments that contained viruses), and the posting of PHI to public websites.

Theft: The largest breach in 2019 resulted from the theft of a laptop containing PHI. The theft affected approximately 112,227 individuals. The most reported cases of theft were of laptops and paper records. In the case of laptops, most incidents resulted from a lack of proper security measures, such as a lack of access controls. For paper records, most incidents involved the burglarizing of offices and storage facilities.

Improper Disposal: The largest reported improper disposal incident in 2019 resulted from housekeeping staff who impermissibly emptied medical records containing PHI into a recycling bin. This breach affected 4,556 individuals. Other improper disposal breaches involved disposing of paper records containing PHI in trash bins rather than authorized shred bins.

Unauthorized Access or Disclosure of PHI: The largest breach in 2019 involving the unauthorized access or disclosure of PHI affected approximately 1,565,338 individuals. In this case, OCR notified a covered entity that the PHI of its patients was accessible via the Internet. Other incidents of unauthorized access or disclosure involved employees impermissibly accessing records outside the scope of their job responsibilities, and misdirected communications.

Loss of PHI: The largest breach reported as a loss in 2019 resulted from the loss of a thumb drive that contained the PHI of approximately 27,004 individuals. Other incidents in this category involved paper and electronic media that could not be located.

Remedial Action Reported

For breaches affecting 500 or more individuals that occurred in 2019, in addition to providing the required notifications, covered entities most commonly reported taking one or more of the following steps to mitigate the potential consequences of the breaches and to prevent future breaches:

- Implementing multi-factor authentication for remote access;
- Revising policies and procedures;
- Training or retraining workforce members who handle PHI;
- Providing free credit monitoring and identity theft protection services to customers;
- Adopting encryption technologies;
- Imposing sanctions on workforce members who violated policies and procedures for removing PHI from facilities or who improperly accessed PHI;
- Changing passwords;
- Performing a new risk assessment; and
- Revising business associate contracts to include more detailed provisions for the protection of health information.

Breaches Involving Fewer than 500 Individuals

A covered entity must notify OCR of breaches involving fewer than 500 individuals no later than 60 days after the end of the calendar year in which the breaches are discovered. For breaches discovered during 2019, notification to OCR was required no later than February 29, 2020.

Breaches involving fewer than 500 individuals for 2019

OCR received 62,771 reports of breaches affecting fewer than 500 individuals during calendar year 2019. These smaller breaches affected 284,812 individuals. Set forth below are the breaches submitted to OCR by covered entity type (in order of frequency):

(1) Health Care Providers (56,495 reports (90%) affecting 222,288 individuals (78%));
(2) Health Plans (4,564 reports (7%) affecting 37,191 individuals (13%));
(3) Business Associates (1,626 reports (3%) affecting 24,566 individuals (9%)); and
(4) Health Care Clearinghouses (86 reports (<1%) affecting 767 individuals (<1%)).

See Figure 7 and 8.

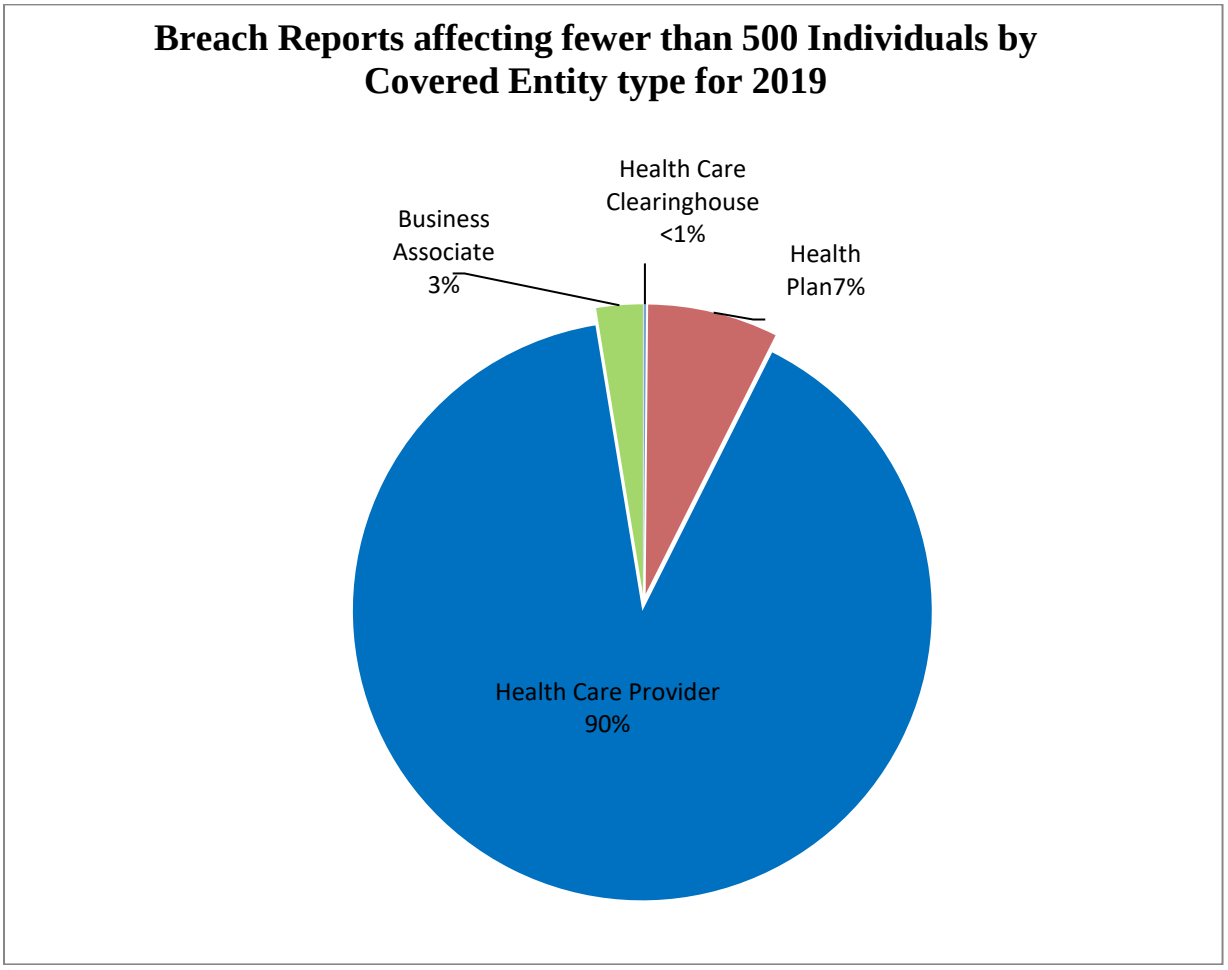

Figure 7

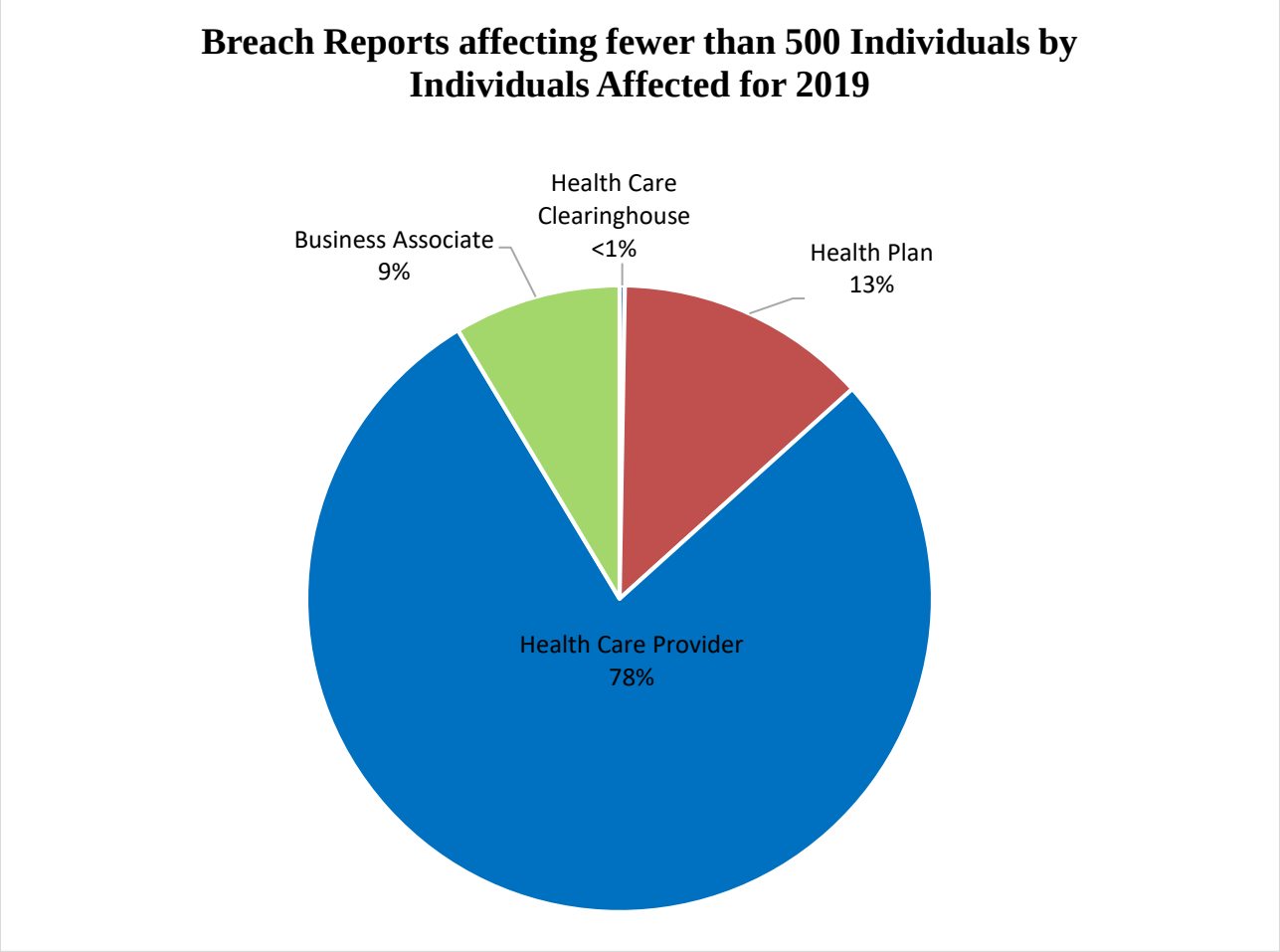

Figure 8

The most common causes of breach incidents (in order of frequency) for breaches affecting fewer than 500 individuals were:

(1) Unauthorized access or disclosure (57,866 reports (92%) affecting 168,095 individuals (59%));
(2) Loss (2,435 reports (4%) affecting 23,554 individuals (8%));
(3) Theft (1,103 reports (2%) affecting 34,313 individuals (12%));
(4) Hacking/IT incident (820 reports (1%) affecting 50,638 individuals (18%)); and
(5) Improper disposal (547 reports (1%) affecting 8,212 individuals (3%)).

See Figures 9 and 10.

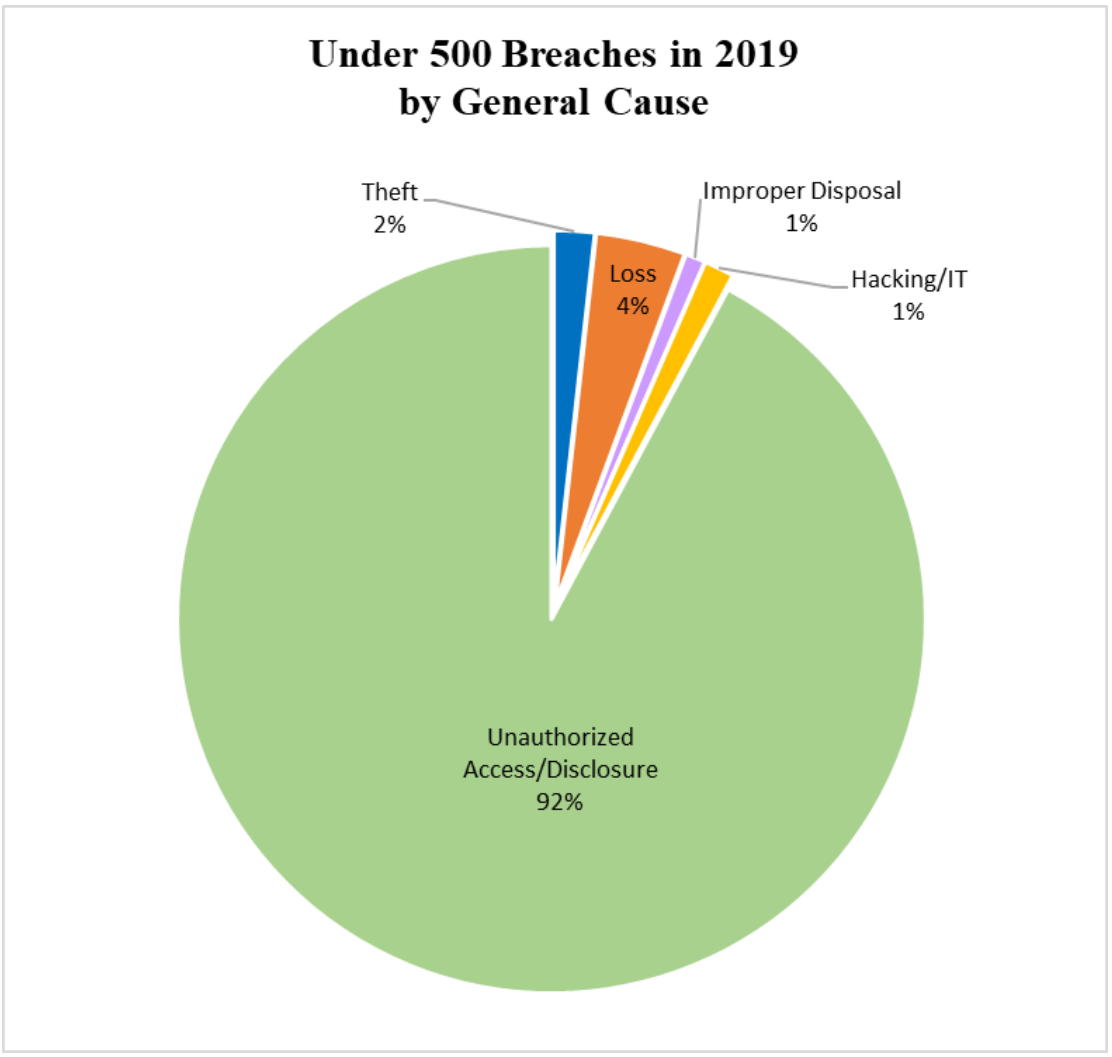
Under 500 Breaches in 2019
by General Cause
Theft
2%
Improper Disposal
1%
Loss
4%
Hacking/IT
1%
Unauthorized
Access/Disclosure
92%

Figure 9

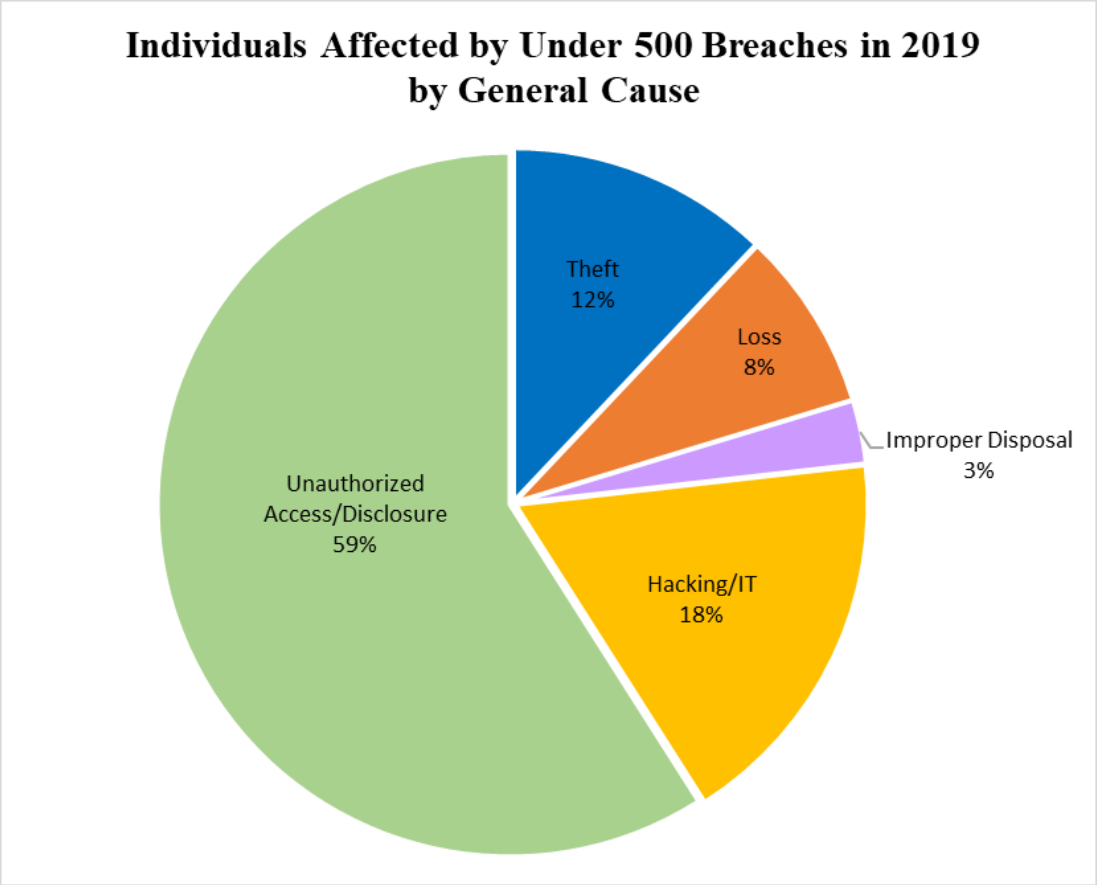

Figure 10

The 62,771 reported breaches affecting fewer than 500 individuals described the following locations of the PHI (in order of frequency):

(1) Paper (42,192 reports (67%) affecting 118,763 individuals (42%));
(2) Electronic medical record (7,807 reports (12%) affecting 28,618 individuals (10%));
(3) Other (7,352 reports (12%) affecting 28,042 individuals (10%));[14]
(4) E-mail (3,111 reports (5%) affecting 70,133 individuals (25%));
(5) Desktop computer (875 reports (1%) affecting 13,597 individuals (5%));
(6) Other portable electronic device (800 reports (1%) affecting 5,942 individuals (2%));
(7) Network server (410 reports (1%) affecting 8,994 individuals (3%)); and
(8) Laptops (224 reports (< 1%) affecting 10,723 individuals (4%)).

See Figures 11 and 12.

[14] See footnote 10 on description of "other" category.

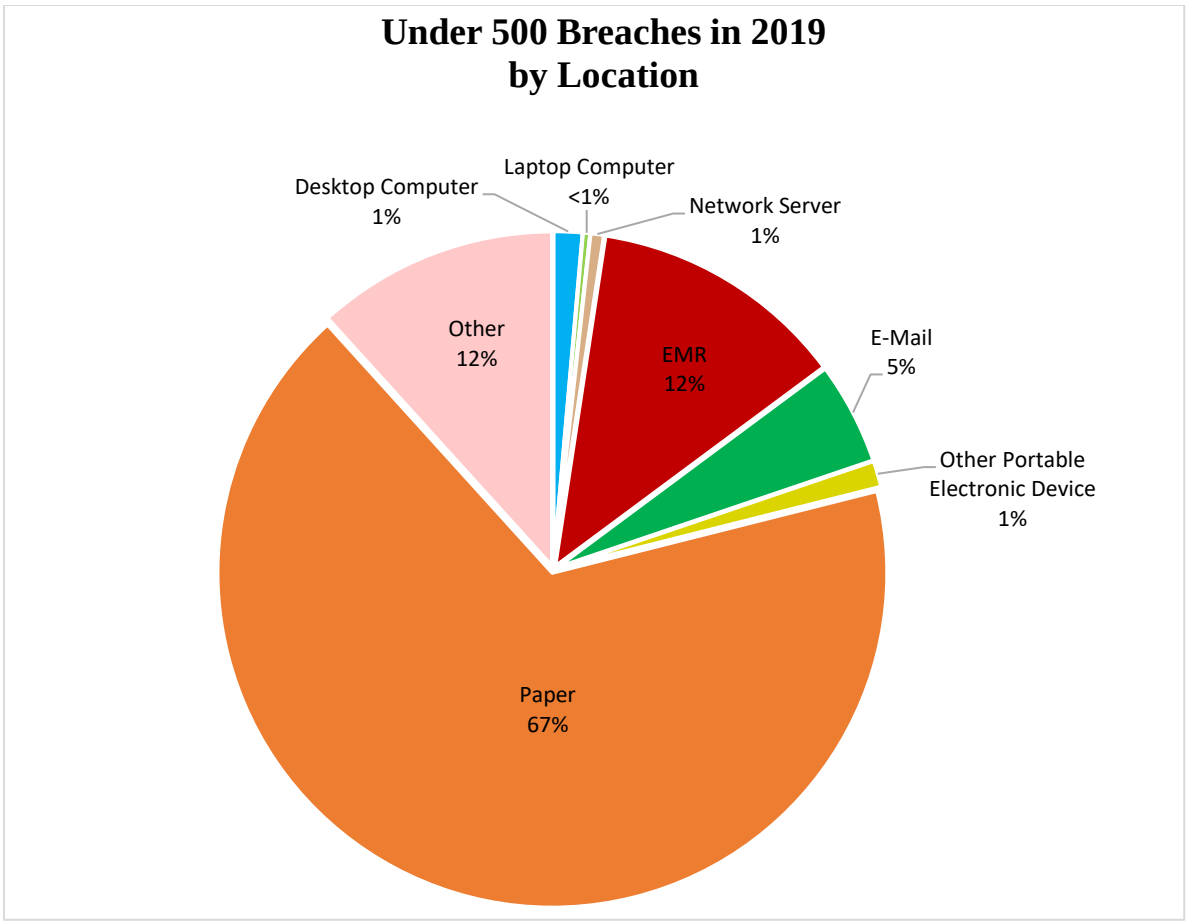
Under 500 Breaches in 2019
by Location
Desktop Computer
1%
Laptop Computer
<1%
Network Server
1%
Other
12%
EMR
12%
E-Mail
5%
Other Portable
Electronic Device
1%
Paper
67%

Figure 11

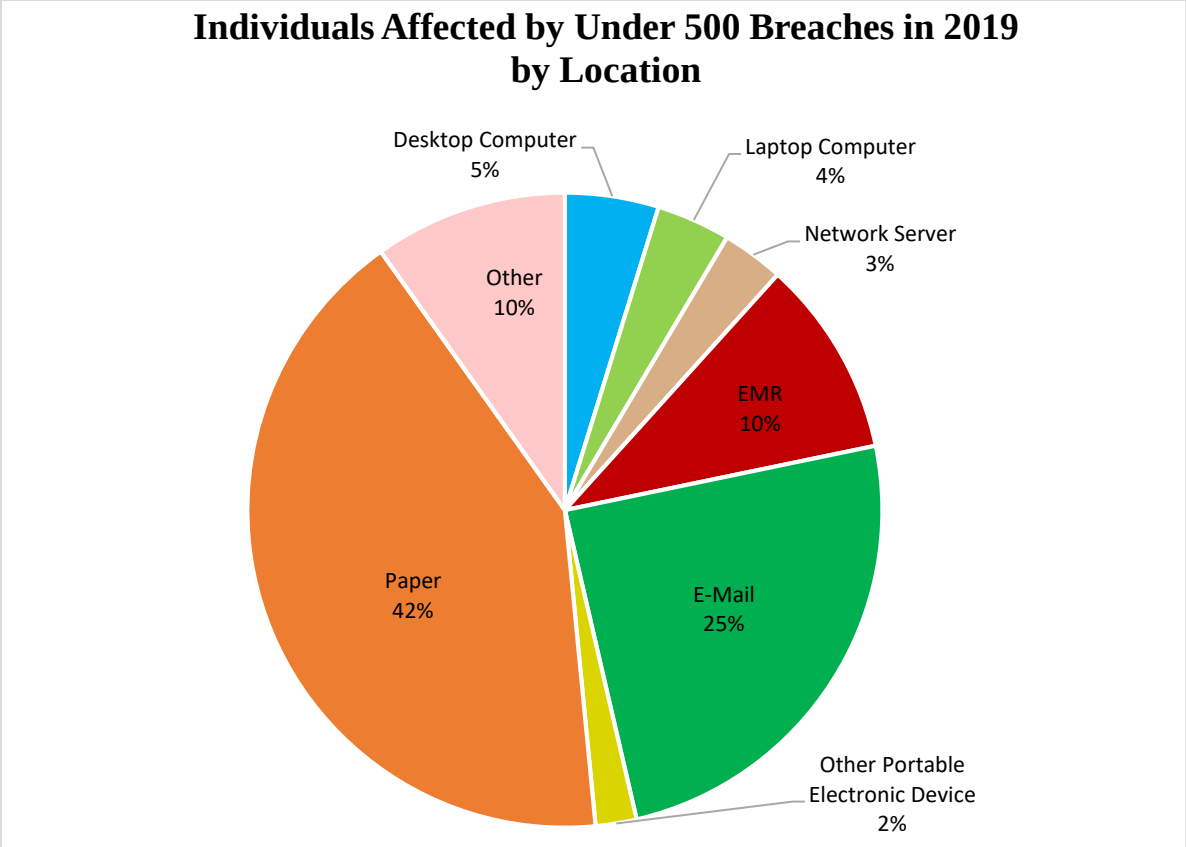

Figure 12

Details on breaches involving fewer than 500 individuals for 2019

As in previous years, incidents reported for 2019 also involved misdirected communications, including incidents where the clinical or claims record of one individual was mistakenly mailed or faxed to another individual, test results were sent to the wrong patient, files were attached to the wrong patient record, emails were sent to the wrong individuals, and member ID cards were mailed to the wrong individuals. In response to these incidents, covered entities commonly reported taking remedial actions such as fixing "glitches" in software that incorrectly compiled lists of patient names and contact information, revising policies and procedures, and training or retraining employees who handle PHI.

In addition to investigating all breaches affecting more than 500 or more individuals, OCR completed 21 breach investigations involving fewer than 500 individuals in 2019.

Cases Investigated and Action Taken

OCR opened investigations into all of the 408 reported breaches affecting 500 or more individuals that occurred in 2019. OCR also opened 20 investigations into breaches affecting fewer than 500 individuals. OCR completed 298 investigations resulting from breach reports after achieving voluntary compliance, through corrective action and technical assistance, through

resolution agreements, or because no violation had occurred. Specific details about the cases that were resolved in 2019 with resolution agreements or civil money penalties can be found at the appendix at the end of this report. Additional information on OCR's compliance and enforcement work may be found in OCR's Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance for Calendar Year 2019.

Lessons Learned

The breach reports submitted to OCR offer insight into areas of vulnerability in protections for the privacy and security of individuals' health information. Covered entities and business associates should consider the following HIPAA Security Rule standards that were identified in OCR investigations in 2019 as areas needing improvement.

- Risk Analysis and Risk Management. HIPAA investigations and resolution agreements from 2019 continued to identify risk analysis and risk management deficiencies among HIPAA covered entities and business associates. Conducting an accurate and thorough assessment of the risks and vulnerabilities to electronic protected health information (ePHI) is a foundational requirement of the HIPAA Security Rule. However, the lack of a proper risk analysis remained a major contributing factor in reported breaches of PHI. Examples of deficient risk analyses from resolution agreements reached in 2019 include entities that did not identify and assess the risk of PHI available over the Internet without a password, did not identify the use of poor passwords and generic logins to access PHI, and did not conduct a risk analysis at all. OCR's investigations also found that even when risks were identified and assessed, some entities took no action or inadequate action to reduce the identified risks as part of its risk management process.

- Access Control. The HIPAA Security Rule requires policies and procedures to be implemented to allow access to PHI only to those persons or software programs that have been granted access rights. However, OCR investigations and resolution agreements in 2019 continued to find evidence of non-compliance with the access control standard that often was a strong contributing factor to a breach of PHI. Examples uncovered during OCR's investigations include multiple instances where access controls were not in place to prevent access to PHI over the Internet to unauthorized individuals and entities. OCR's investigations also found that a lack of access controls, particularly access to network resources and privileged accounts, can contribute to the escalation and prolonging of malicious intrusions by hackers and malicious software, including ransomware.

- Encryption and Decryption. Even as cyberattacks proliferate across the health care sector, lost and stolen devices continue to be a source of breaches of PHI. One laptop or smartphone can contain the PHI of potentially thousands or even millions of individuals. The HIPAA Security Rule requires entities to consider encryption as a solution to protect ePHI where it is reasonable and appropriate to do so. One area in which encryption is most likely reasonable and appropriate is to protect ePHI stored on portable devices (*e.g.*, laptops, smartphones, and USB devices). However, OCR's investigations and resolution agreements from 2019 found multiple instances of lost and stolen laptops and USB

devices containing unencrypted PHI. Although an analysis of OCR's breach reports shows an overall decrease in the number of reported breaches due to lost or stolen portable devices over the past several years, such breaches continue; yet, these breaches are easily prevented using readily available and inexpensive encryption solutions.

- Information System Activity Review. Timely review of information system activity is one means by which entities can be alerted to a potential breach of ePHI. HIPAA regulated entities are required to regularly review information system activity such as audit logs, access reports and security incident tracking reports. However, OCR's investigations in 2019 found multiple instances of poor or non-existent information system activity review processes that contributed to breaches of ePHI by external hackers and malicious insiders. In one instance, a hospital employee's impermissible access of patients' ePHI went undetected for approximately five years. In another, a hacker accessed several databases undetected and was able to exfiltrate the ePHI of a large number of individuals. Effective information system activity review processes can identify potential malicious activity from both internal and external sources. Early detection of malicious activity is key to halting potential breaches and mitigating the number of individuals affected.

- Audit Controls. The number of breaches due to hacking or IT incidents continues to be the most common breach reported to OCR (affecting 500 or more individuals). If a malicious actor or malware (such as ransomware) gains access to an entity's information technology systems, it is critical that audit logs are enabled and properly configured to record and track malicious activities. Entities regulated by HIPAA are required to implement mechanisms to record and examine activity in systems that contain or use ePHI. However, investigations conducted and resolution agreements reached during 2019 have uncovered numerous deficiencies by HIPAA covered entities and business associates in maintaining proper audit logs. Examples include not implementing audit logs at all, and misconfigurations that do not capture the information necessary to examine user or system activity.

- Response and Reporting. Entities regulated by HIPAA are required to respond to and mitigate the harmful effects of security incidents[15] as well as document security incidents and their outcomes. Entities should be prepared to effectively respond to a variety of security incidents (*e.g.*, malicious insiders, ransomware, advanced persistent threats). However, resolution agreements and investigations from 2019 show that some entities failed to respond to security incidents. For example, in one instance an entity was warned by the FBI and OCR that PHI from its organization was available over the Internet, yet the entity's response and subsequent investigation determined that no PHI was impacted by the incident. Only during the course of OCR's investigation and responding to OCR's data requests did the entity subsequently determine that PHI was in fact impacted by the

[15] A security incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. 45 CFR § 164.304. A breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under [the Privacy Rule] which compromises the security or integrity of the protected health information. 45 CFR § 164.402.

security incident. The initial ineffective response led to a delay in notifications to individuals whose PHI was affected by the breach.

Summary and Conclusion

As in 2018, hacking/IT incidents was the largest category of breaches occurring in 2019 involving 500 or more individuals, and also affected the most individuals. Additionally, email continues to be the largest category by location for breaches involving 500 or more individuals. For the under 500 breaches that occurred in 2019, unauthorized disclosures were the largest category of type of breach report, and paper records were the largest category by location.

The breach notification requirements are achieving their objectives of increasing public transparency and accountability of covered entities and business associates. The reports submitted to OCR show that millions of affected individuals are receiving notifications of breaches. To provide increased public transparency, information about breaches involving 500 or more individuals is available for public view on the OCR website at http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html. The breaches are posted in an accessible format that allows users to search and sort the posted breaches by name of covered entity, name of business associate (if applicable), state, number of individuals affected, date of breach, type of breach, and location of the breached information (*e.g.*, laptop computer). Additionally, the website provides brief summaries of the enforcement cases, including cases stemming from a breach report that OCR has investigated and closed.

OCR continues to exercise its oversight responsibilities by reviewing and responding to breach notification reports and initiating investigations into all breaches involving 500 or more individuals, as well as into a number of breaches involving fewer than 500 individuals. During 2019, in five cases resulting from breach reports, OCR entered into resolution agreements/corrective action plans or imposed civil money penalties totaling more than $6.9 million.[16]

[16] The five cases were Medical Informatics Engineering, Jackson Health System, Texas Health and Human Services Commission, University of Rochester Medical Center, and West Georgia Ambulance.

APPENDIX

Resolution Agreements and Civil Money Penalties in 2019

Resolution Agreement with Medical Informatics Engineering

Medical Informatics Engineering, Inc. (MIE) agreed to pay $100,000 and take corrective action to settle potential violations of the HIPAA Privacy and Security Rules. MIE is an Indiana company that provides software and electronic medical record services to healthcare providers.

On July 23, 2015, MIE filed a breach report with OCR following discovery that hackers used a compromised user ID and password to access the ePHI of approximately 3.5 million people.

OCR's investigation revealed that MIE failed to conduct a comprehensive risk analysis to assess the potential risks and vulnerabilities to the confidentiality, integrity, and availability of its ePHI.

In addition to the monetary settlement, MIE agreed to:

- Complete an enterprise-wide risk analysis; and
- Develop and implement a risk management plan.

This settlement occurred in April 2019.

Civil Money Penalty imposed on Jackson Health System

OCR imposed a civil money penalty of $2,154,000 against Jackson Health System (JHS) for violations of the HIPAA Security and Breach Notification Rules between 2013 and 2016. JHS is a nonprofit academic medical system based in Miami, Florida, which operates six major hospitals, a network of urgent care centers, multiple primary care and specialty care centers, long-term care nursing facilities, and corrections health services clinics. JHS provides health services to approximately 650,000 patients annually and employs about 12,000 individuals.

On August 22, 2013, JHS submitted a breach report to OCR stating that its health information management department had lost paper records containing the PHI of 756 patients in January 2013. JHS's internal investigation determined that an additional three boxes of patient records were also lost in December 2012; however, JHS did not report the additional loss or the increased number of individuals affected to 1,436, until June 7, 2016.

In July 2015, OCR initiated an investigation following a media report that disclosed the PHI of a JHS patient. A reporter had shared a photograph of a JHS operating room screen containing the patient's medical information on social media. JHS subsequently determined that two employees had accessed this patient's electronic medical record without a job-related purpose.

On February 19, 2016, JHS submitted a breach report to OCR reporting that an employee had been selling patient PHI. The employee had inappropriately accessed over 24,000 patients' records since 2011.

OCR's investigation revealed that JHS failed to provide timely and accurate breach notification to the Secretary, conduct enterprise-wide risk analyses, manage identified risks to a reasonable

and appropriate level, regularly review information system activity records, and restrict authorization of its workforce members' access to patient ePHI to the minimum necessary to accomplish their job duties.

JHS waived its right to a hearing and did not contest the findings in OCR's Notice of Proposed Determination. Accordingly, OCR issued a Notice of Final Determination and JHS paid the full civil money penalty.

This action occurred in October 2019.

Civil Money Penalty imposed on Texas Health and Human Services Commission

OCR imposed a $1,600,000 civil money penalty against the Texas Health and Human Services Commission (TX HHSC), for violations of the HIPAA Privacy and Security Rules between 2013 and 2017. TX HHSC is part of the Texas HHS system, which operates state supported living centers; provides mental health and substance use services; regulates child care and nursing facilities; and administers hundreds of programs for people who need assistance, including supplemental nutrition benefits and Medicaid. The Department of Aging and Disability Services (DADS), a state agency that administered long-term care services for people who are aging, and for people with intellectual and physical disabilities, was reorganized into TX HHSC in September 2017.

On June 11, 2015, DADS filed a breach report with OCR stating that the ePHI of 6,617 individuals was viewable over the internet, including names, addresses, social security numbers, and treatment information. The breach occurred when an internal application was moved from a private, secure server to a public server and a flaw in the software code allowed access to ePHI without access credentials. OCR's investigation determined that, in addition to the impermissible disclosure, DADS failed to conduct an enterprise-wide risk analysis and implement access and audit controls on its information systems and applications as required by the HIPAA Security Rule. Because of inadequate audit controls, DADS was unable to determine how many unauthorized persons accessed individuals' ePHI.

TX HHSC waived its right to a hearing and did not contest the findings in OCR's Notice of Proposed Determination. Accordingly, OCR issued a Notice of Final Determination and TX HHSC paid the full civil money penalty.

This action occurred in October 2019.

Resolution Agreement with University of Rochester Medical Center

The University of Rochester Medical Center (URMC) agreed to pay $3 million and take corrective action to settle potential violations of the HIPAA Privacy and Security Rules. URMC includes healthcare components such as the School of Medicine and Dentistry and Strong Memorial Hospital. URMC is one of the largest health systems in New York State with over 26,000 employees.

URMC filed breach reports with OCR in 2013 and 2017 following its discovery that PHI had been impermissibly disclosed through the loss of an unencrypted flash drive and theft of an unencrypted laptop, respectively. OCR's investigation revealed that URMC failed to:

- Conduct an enterprise-wide risk analysis;
- Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level;
- Utilize device and media controls; and
- Employ a mechanism to encrypt and decrypt ePHI when it was reasonable and appropriate to do so.

Of note, in 2010, OCR investigated URMC concerning a similar breach involving a lost unencrypted flash drive and provided technical assistance to URMC. Despite the previous OCR investigation, and URMC's own identification of a lack of encryption as a high risk to ePHI, URMC permitted the continued use of unencrypted mobile devices.

In addition to the monetary settlement, URMC agreed to:

- Conduct an enterprise-wide risk analysis;
- Develop and implement a risk management plan;
- Implement a process for evaluating environmental and operational changes;
- Develop, maintain, review, and revise, if necessary, HIPAA Privacy and Security Rule policies and procedures; and
- Train workforce members on HIPAA Privacy and Security Rule policies and procedures.

This settlement occurred in October 2019.

Resolution Agreement with West Georgia Ambulance

West Georgia Ambulance, Inc. (West Georgia), agreed to pay $65,000 and take corrective action to settle potential violations of the HIPAA Security Rule. West Georgia is an ambulance company that provides emergency and non-emergency ambulance services in Carroll County, Georgia.

OCR began its investigation after West Georgia filed a breach report in 2013 concerning the loss of an unencrypted laptop containing the PHI of 500 individuals. OCR’s investigation uncovered long-standing noncompliance with the HIPAA Rules, including failures to:

- Conduct an accurate and thorough risk analysis of potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI;
- Failure to adopt and implement a security awareness and training program; and
- Failure to implement HIPAA Security Rule policies and procedures.

In addition to the monetary settlement, West Georgia will:

- Conduct an enterprise-wide risk analysis;
- Develop and implement a risk management plan;

- Adopt and implement written policies and procedures to comply with the HIPAA Privacy, Security, and Breach Notification Rules;
- Train workforce members on the revised policies and procedures;
- Identify all business associates and provide copies of business associate agreements to OCR;
- Install HIPAA compliant encryption software on all of its computers; and
- Revise its HIPAA Notice of Privacy Practices.

This settlement occurred in December 2019.