Australian Government

Office of the Australian Information Commissioner

Annual report of the Australian Information Commissioner's activities in relation to digital health 2022–23

OAIC

Annual report of the Australian Information Commissioner's activities in relation to digital health 2022–23

The Office of the Australian Information Commissioner (OAIC) was established on 1 November 2010 by the *Australian Information Commissioner Act 2010*.

ISSN 2202–7262

Creative commons

This publication should be attributed as:

Office of the Australian Information Commissioner, *Annual report of the Australian Information Commissioner's activities in relation to digital health 2022–23*.

Contact

Enquiries regarding the licence and any use of this report are welcome.

Email: corporate@oaic.gov.au
Website: oaic.gov.au
Phone: 1300 363 992

Mail: Director, Strategic Communications
Office of the Australian Information Commissioner
GPO Box 5288
Sydney NSW 2001

Non-English speakers

If you speak a language other than English and need help, please call the Translating and Interpreting Service on 131 450 and ask for the Office of the Australian Information Commissioner on 1300 363 992.

Accessible formats

All our publications can be made available in a range of accessible formats. If you would like this report in an accessible format, please contact us.

Acknowledgment of Country

The OAIC acknowledges Traditional Custodians of Country across Australia and recognises their continuing connection to lands, waters and communities. We pay our respect to Aboriginal and Torres Strait Islander cultures and to Elders past and present.

Contents

Executive summary

This annual report sets out the Australian Information Commissioner's digital health compliance and regulatory activity during 2022–23, in accordance with section 106 of the *My Health Records Act 2012* (My Health Records Act) and section 30 of the *Healthcare Identifiers Act 2010* (HI Act).

Digital health is an increasingly significant part of the healthcare system, and while the use of digital health information continues to grow, it is it is critical that privacy measures are upheld.

The Australian Government has established two key services to underpin digital health in Australia: the Healthcare Identifiers Service (HI Service), and the My Health Record system. Both involve the management of personal information – and for the purposes of this report, we refer to them collectively as 'digital health'.

Healthcare identifiers are assigned to individuals, healthcare providers, and healthcare provider organisations. They help healthcare providers communicate accurately with each other and identify and access patient records in the My Health Record system.

The My Health Record system is an online summary of an individual's health information, including their medicines, immunisations, allergies and medical history. Registered healthcare providers, including doctors, nurses and allied health professionals involved in their care can view and add information to it, subject to legislative obligations and any individual access controls.

Following the earlier establishment of the HI Service, the My Health Record system commenced in 2012 as an opt-in system: people needed to register in order to establish and share their record. In 2017, the Australian Government announced the creation of a My Health Record for every Australian. Following an opt-out period that ended on 31 January 2019, a My Health Record was created for everyone who had not opted out of the system.

Privacy is critical to ensuring trust in digital health, and the legislation establishing the My Health Record system and HI Service include important privacy provisions, which are regulated by the Office of the Australian Information Commissioner (OAIC). These provisions recognise the special sensitivity of health information, and protect and restrict its collection, use and disclosure. We work to ensure that healthcare providers understand and comply with their privacy obligations.

This report provides information about digital health activities undertaken by the OAIC, including our assessment program, handling of My Health Record data breach notifications, development of guidance material, provision of advice, and liaison with key stakeholders.

In 2022–23, the OAIC received 10 privacy complaints relating to the My Health Record system with 11 complaints ongoing at the end of the reporting period, including 6 complaints received in previous reporting periods. We finalised 8 My Health Record system complaints, including 3 complaints from previous reporting periods.

We received 5 new privacy complaints relating to the HI Service in 2022–23, of which we finalised 1, as well as another 7 complaints from the previous year.

Over the reporting period, the OAIC has continued its focus on regulatory policy work in relation to the HI Service and continued to handle complaints and enquiries about healthcare identifiers. These complaints and enquiries primarily concerned the inclusion of Individual Healthcare Identifiers (IHIs) on COVID-19 digital vaccination certificates (vaccination certificates). On 3 December 2022, IHIs were removed from vaccination certificates and we updated our published privacy guidance to assist entities and individuals who had collected vaccination certificates containing an IHI.

We received 10 data breach notifications during the reporting period in relation to the My Health Record system and closed 10 notifications.

We also carried out other digital health-related work including:

- commencing one assessment regarding the My Health Record system and finalising 2 further assessments as part of the My Health Record access security policy assessment program
- providing advice to stakeholders, including the Australian Digital Health Agency (ADHA), Services Australia and the Department of Health and Aged Care about privacy-related matters relevant to the My Health Record system and HI Service
- developing and promoting guidance materials, including publishing a template for healthcare providers to help them comply with security and access policy requirements under the My Health Records Rule 2016 and updating our My Health Record emergency access function guidance
- engaging with the Department of Health and Aged Care regarding the proposed amendments to the Healthcare Identifiers Regulations 2020 and the HI Act, and
- monitoring developments in the My Health Record system and the HI Service.

Part 1
Introduction

Many Australians view their health information as being particularly sensitive. This sensitivity has been recognised in the My Health Records Act and HI Act, which regulate the collection, use and disclosure of information, and give the Information Commissioner a range of enforcement powers. This sensitivity is also recognised in the *Privacy Act 1988* (Privacy Act) which treats health information as 'sensitive information'.

Regulatory work of the OAIC

The Australian Information Commissioner (Information Commissioner) is the independent regulator of the privacy provisions relevant to the My Health Record system and HI Service. In addition to this compliance and enforcement role, the OAIC performs proactive education and guidance functions. In 2022–23, the OAIC's regulatory work included:

- regulatory oversight of the My Health Record system, including responding to enquiries and complaints, handling data breach notifications, providing privacy advice and conducting privacy assessments and investigations
- publishing and promoting a template for healthcare providers to help them comply with security and access policy requirements under the My Health Records Rule 2016.
- collaborating with the ADHA to produce an e-Learning module to support users of the OAIC's security and access policy template
- updating guidance about the My Health Record emergency access function.
- updating privacy guidance regarding IHIs on COVID-19 digital vaccination certificates.
- responding to the Department of Health and Aged Care regarding the proposed amendments to the Healthcare Identifiers Regulations 2020
- engaging with the Department of Health and Aged Care regarding proposed amendments to the HI Act, and
- providing feedback about the design of the My Health Record Research and Public Health scheme as part of the proof of concept.

Funding

Prior to 1 July 2021, the OAIC was funded to undertake activities related to both the My Health Record system and the HI Service by a Memorandum of Understanding with the ADHA. From 1 July 2021, the OAIC received a direct appropriation for our role as the independent privacy regulator for the My Health Record system and the HI Service and there was no longer an MOU arrangement between the OAIC and the ADHA.

Year in review summary

The table below summarises the digital health activities (relating to the My Health Record system and the HI Service) undertaken by the OAIC during the 2022–23 financial year.

Table 1: OAIC My Health Record and HI Service activities 2022–23

Activity	My Health Record	HI Service
Telephone enquiries	9	1
Written enquiries	4	3
Complaints received	10	5
Complaints finalised	8	8
Commissioner-investigated investigations finalised	18	0
Regulatory policy advices	34	13
Assessments completed or in progress	3	0
Data breach notifications received	10	N/A
Data breach notifications finalised	10	N/A
Media enquiries	0	0

* A complaint may cover more than one issue. N/A is listed for data breach notifications for the HI Service because there are no mandatory data breach reporting requirements under the HI Act.

Part 2
The OAIC and the My Health Record system

The OAIC performs a range of functions in relation to the My Health Record system. These functions include legislative compliance and regulatory and other activities such as providing privacy-related advice and developing guidance materials for internal and external stakeholders.

The Information Commissioner has the following roles and responsibilities under the My Health Records Act and the Privacy Act:

- respond to complaints received relating to the privacy aspects of the My Health Record system, including through preliminary inquiries, conciliation, investigation or deciding not to investigate a complaint
- investigate, on the Commissioner's own initiative, acts and practices that may be a contravention of the My Health Records Act in connection with health information contained in a healthcare recipient's My Health Record or a provision of Part 4 or 5 of the My Health Records Act
- receive data breach notifications and assist affected entities to deal with data breaches in accordance with the My Health Record legislative requirements
- investigate failures to notify data breaches
- exercise, as the Commissioner considers appropriate, a range of enforcement powers available in relation to contraventions of the My Health Records Act or contraventions of the Privacy Act relating to the My Health Record system, including making determinations, accepting enforceable undertakings, seeking injunctions and seeking civil penalties
- conduct assessments of participants in the system to ensure they are complying with their privacy obligations
- produce statutory and regulatory guidance for consumers and other participants such as healthcare providers, registered repository operators and the ADHA
- maintain guidance for exercising the powers available to the Commissioner in relation to the My Health Record system.

We also respond to enquiries and requests for regulatory policy advice from a broad range of stakeholders about the privacy framework for the My Health Record system and the appropriate handling of My Health Record information. These activities are an important component of the OAIC's regulatory role under the My Health Record system.

The OAIC liaises with external stakeholders, including professional industry bodies in the health sector in the course of handling enquiries and providing regulatory policy advice. Information about the OAIC's activities in relation to providing advice, developing guidance material and liaison with key stakeholders is provided below.

OAIC compliance and regulatory activities

Complaints and investigations relating to the My Health Record system

The OAIC received 10 complaints about the My Health Record system during 2022-23, which is a decrease of 29% on the previous year. We finalised 5 out of the 10 complaints received about the My Health Record system, as well as another 3 complaints from 2021-22.

The Information Commissioner commenced and finalised 18 Commissioner-initiated investigations relating to the My Health Record system during this reporting period. [1] The investigations were commenced in respect of 18 healthcare provider organisations (HPOs) who were registered for access to the My Health Record system. The OAIC investigated their compliance with the requirement to have in place a written security and access policy pursuant to Rule 42(1) of the My Health Record Rule 2016 which reasonably addresses the items specified in Rule 42(4).

Assessments relating to the My Health Record system

In the 2022-23 financial year, the OAIC commenced one assessment regarding the My Health Record system and finalised 2 further assessments as part of the My Health Record access security policy assessment program.

Table 2: Assessments relating to the My Health Record system conducted in 2022-23

Assessment subject	Number of entities assessed	Year opened	Status
My Health Records Assessment 1: Assessment of general practice clinics – APPs 1.2 and 11, and Rule 42 My Health Records Rule 2016	300	2020–21	Complete
My Health Records Assessment 2: Assessment of general practice clinics – APPs 1.2 and 11, and Rule 42 My Health Records Rule 2016	20	2021–22	Complete
Assessment of a mobile health application – APPs 1.2-1.4 and 5	1	2022-23	Ongoing

[1] When an investigation is finalised, it may be closed, or referred to the Determinations team for consideration, and a determination, litigation or enforceable undertaking may follow.

Assessment snapshots

My Health Records Assessment 1

In the first My Health Record assessment, the OAIC surveyed 300 general practice (GP) clinics across Australia to assess compliance with the requirements of Rule 42 of the My Health Records Rule 2016, which requires entities to have a security and access policy. Compliance with Rule 42 is a reasonable step the OAIC expects health service providers to take when securing personal information they collect and hold under Australian Privacy Principle (APP) 11.1.

This assessment found that over two-thirds of GP clinics that responded to the survey had a security and access policy. However, over 30% of survey respondents did not provide a security and access policy when requested.

After the survey had closed, the OAIC contacted GP clinics that did not provide a security and access policy in the survey. At the conclusion of this process, 79% of the 300 GPs[1] had provided a security and access policy – up from 59% at the time of the survey.

You can read the full report on our website.[2]

Following the assessment the OAIC conducted Commissioner-initiated iInvestigations into those clinics who did not have a security and access policy.

My Health Records Assessment 2

In 2022-23, the OAIC finalised an assessment of 20 GP clinics across Australia (selected from the 300 GP clinics in Assessment 1). The OAIC examined these GP clinics' governance arrangements, in particular their security and access policy, and identified any privacy risks relating to Rule 42 of the My Health Records Rule 2016, and APPs 1.2 and 11.

Although most of the GP clinics assessed were aware of the requirement to have a security and access policy, it was unclear how well they understood the substantive requirements and purpose of Rule 42. Recommendations were made to each GP clinic across a number of areas including staff training, access, security and risk, and document management. For example, the assessment found that nearly half of the assessed GPs did not follow best practice password requirements and 14 of the 20 security and access policies assessed did not address required strategies for identifying, acting upon and reporting My Health Record system-related security risks.

You can read the full report on our website.[3]

Following the assessment, the OAIC published the OAIC security and access policy template, which is available on our website.[4]

Assessment of a mobile health application

In 2022-23, the OAIC commenced an assessment of a mobile application that can be used to access the My Health Record system. This assessment will assess the handling of personal information through the mobile application under APPs 1.2, 1.3, 1.4 and 5. This assessment is expected to be finalised in 2023–24 and an assessment report will be published on the OAIC website.

[1] Forty-two GP clinics failed to provide a response to the survey and therefore did not participate in this assessment
[2] www.oaic.gov.au/myhealthrecord-assessment1
[3] www.oaic.gov.au/myhealthrecord-assessment2
[4] www.oaic.gov.au/myhealthrecord-rule42guide

Data breach notifications

In 2022–23, the OAIC received 10 data breach notifications in relation to the My Health Record system and closed 10 notifications.

Table 3: Data breach notifications 2022–23

	Notified in the period			Closed in the period		
Notifying party	**No. of data breach notifications**	**No. of healthcare recipients affected**	**No. of affected recipients holding a My Health Record**	**No. of data breach notifications**	**No. of healthcare recipients affected**	**No. of affected recipients holding a My Health Record**
ADHA	1	42	42	1	42	42
Services Australia	0	0	0	0	0	0
Healthcare provider organisations	9	20	20	9	20	20

My Health Record system advice, guidance, liaison and other activities

Advice

My Health Record system enquiries

The OAIC's enquiries team received 9 telephone enquiries and 4 written enquiries about the My Health Record system during the reporting period.

Regulatory policy advice to stakeholders

During the reporting period, the OAIC provided 34 pieces of regulatory policy advice to various stakeholders related to the My Health Record system. These included:

- engagement in relation to the design of the My Health Record Research and Public Health scheme as part of the proof of concept
- providing advice to the Department of Health and Aged Care on the designation process under section 110 of the My Health Records Act
- providing advice to ADHA and Australian Institute of Health and Welfare regarding secondary use of My Health Record data and the National Health (Privacy) Rules.

Regulatory policy advice to the ADHA

The OAIC liaised and coordinated with the ADHA on privacy-related matters relating to the My Health Record system. During the reporting period, this included:

- reviewing and providing feedback on the ADHA's e-Learning module to accompany the security and access policy template
- meeting with ADHA to discuss supplementary guidance for sole traders using the security and access policy template
- providing advice to ADHA about the formalisation of an escalation pathway for higher risk My Health Record matters.

Guidance

For health service providers

The OAIC's guidance focus in 2022-23 was publishing a security and access policy template to help healthcare providers comply with their obligations under Rule 42 of the My Health Records Rule 2016 (Rule 42) and new Rule 42 guidance.

Rule 42 requires healthcare provider organisations to have, communicate and enforce a written security and access policy in order to register, and remain registered, to use the My Health Record system.

The OAIC worked closely with the ADHA to develop a template that is available for download as a customisable Word document. The template was informed by the OAIC's assessments of Rule 42 compliance and stakeholder feedback received through consultation with clinical peak bodies, primary health networks and ADHA clinical leads.

The template is supported by new OAIC Rule 42 guidance, including new tips to help healthcare providers develop, implement and maintain an effective security and access policy and associated governance. The OAIC also provided input to the ADHA's new e-Learning course to further assist users of the template.

The OAIC monitored use of the template and has collaborated with the ADHA in refreshing its design to increase its effectiveness. The updated template will be available for download early in the 2023-24 financial year.

A new My Health Record notifiable data breaches form is under development, in conjunction with a new website landing page containing information for participants in the My Health Record system about their notification obligations.

The OAIC also updated our My Health Record emergency access function guidance.

For consumers

The OAIC website features a dedicated health information privacy section for individuals, including privacy advice for the My Health Record system. My Health Record privacy advice is also highlighted through a microsite which features FAQs, a video and information on how to make a complaint.

Liaison

Liaison with the ADHA

The OAIC liaised regularly with the ADHA to discuss privacy matters relating to the My Health Record system and guidance projects.

Other activities

Monitoring developments in digital health and the My Health Record system

The OAIC actively monitors developments in digital health to inform its regulatory role. During the reporting period, staff attended:

- the annual Digital Health Institute Summit on 17-18 October 2022. The conference was organised by Australasian Institute of Digital Health and e-Health NSW focussing on healthcare strategies in a digital world.
- an online workshop on 15 November 2022 hosted by the University of Melbourne concerning regulatory pathways that exist under the National Safety and Quality Digital Mental Health Standards.
- an online information session on 7 March 2023 hosted by the Australasian Institute of Digital Health regarding the Digital Health Capability Action Plan (CAP). The CAP sets out the initiatives planned over a two-year period to equip Australia's health workforce for a connected, digitally enabled future.
- Australian Healthcare Week on 15 March 2023 to engage in relation to interoperability standards, privacy and changing consumer expectations around healthcare and digital innovation.
- the Digital Health Festival on 6 and 7 June 2023 to learn about new healthcare technologies and innovations in a time of rapid digital health technology adoption.
- Queensland Healthcare Week on 28 June 2023. The online event focussed on future-proofing hospital infrastructure, operations and services.

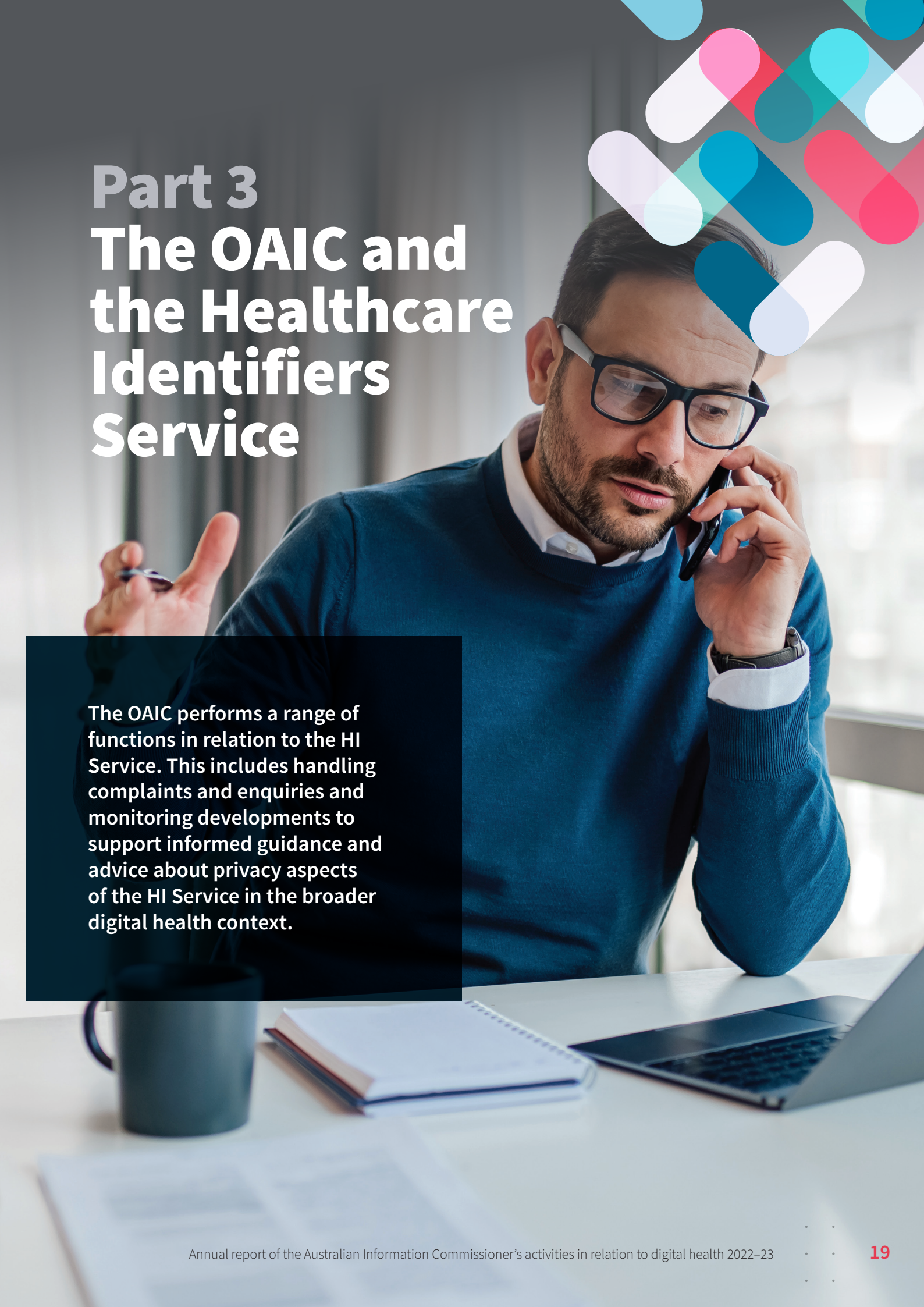
Presentations

- The OAIC provided a presentation on 'Health and technology and the importance of building trust through privacy' at the Medical Software Industry Association Summit on 3 November 2022.
- As part of the Australian Commission on Safety and Quality in Health Care's launch of the Digital Mental Health Standards accreditation scheme in November this year, the OAIC presented at a webinar aimed at digital mental health service providers, service users and other stakeholders. The session focussed on privacy, information and cyber security and took place on 21 February 2023.

Submissions

- The OAIC provided a submission to the Department of Health and Aged Care on the Consultation Regulatory Impact Statement on general practice data and electronic clinical decision support on 14 March 2023.

Part 3
The OAIC and the Healthcare Identifiers Service



The OAIC performs a range of functions in relation to the HI Service. This includes handling complaints and enquiries and monitoring developments to support informed guidance and advice about privacy aspects of the HI Service in the broader digital health context.

The OAIC is the independent regulator of the privacy aspects of the HI Act and the Healthcare Identifiers Regulations 2020.

The HI Act implements a national system for assigning unique identifiers to individuals, healthcare providers, and healthcare provider organisations. The identifiers are assigned and administered through the HI Service, currently operated by the Chief Executive of Medicare.

The HI Service is a foundation service for a range of digital health initiatives in Australia, particularly the My Health Record system. Under the My Health Record system, healthcare identifiers:

- are used to identify healthcare recipients who register for a My Health Record
- enable the ADHA to authenticate the identity of all individuals who access a My Health Record and record activity through the audit trail
- help ensure the correct health information is associated with the correct healthcare recipient's My Health Record.
- There are three types of healthcare identifiers issued by the HI Service, namely:
- Individual Healthcare Identifiers (IHI) — for individuals receiving healthcare in Australia
- Healthcare Provider Identifier – Individual (HPI-I) — for individual healthcare providers, such as GPs, allied health professionals, nurses, dentists and pharmacists
- Healthcare Provider Identifier – Organisation (HPI-O) — for organisations delivering healthcare, such as hospitals and general practices.

The HI Act imposes a high standard of privacy on healthcare identifiers, and they may only be accessed, used and disclosed for limited purposes.

Registration with the HI Service is a prerequisite for a healthcare provider organisation to be registered for the My Health Record system.

The Information Commissioner has the following roles and responsibilities under the HI Act and the Privacy Act:

- respond to complaints received relating to the privacy aspects of the HI Service, including through preliminary inquiries, conciliation, investigation or deciding not to investigate a complaint
- investigate, on the Commissioner's own initiative, acts and practices that may be a misuse of healthcare identifiers
- receive data breach notifications and respond as appropriate
- conduct assessments
- provide a range of regulatory policy advice and guidance material.

OAIC compliance and regulatory activities

Complaints relating to the Healthcare Identifiers Service

The OAIC received 5 complaints about healthcare identifiers in 2022-23, which is down 62% on the previous year. We finalised 1 out of the 5 complaints received, as well as another 7 complaints from the previous year.

All of the complaints finalised by the OAIC were done so prior to any formal investigation being undertaken.

Investigations relating to the Healthcare Identifiers Service

No complaint investigations or Commissioner-initiated investigations were commenced or finalised in this reporting period. As at 30 June 2023, there were no HI Service investigations open.

Assessments relating to the Healthcare Identifiers Service

The OAIC did not initiate any assessments of the HI Service in 2022–23. The digital health assessment program for the 2022-23 financial year focused on privacy obligations related to the My Health Record system.

HI Service advice, guidance, liaison and other activities

Advice

HI Service enquiries

The OAIC's enquiries team received 1 phone enquiry, and 3 written enquiries about the handling of healthcare identifiers during the reporting period.

Regulatory policy advice to stakeholders

In relation to the HI Service, the OAIC provided 13 pieces of regulatory policy advice during the reporting period. Some examples of advice provided in relation to the HI Service include:

- providing advice to the Department of Health and Aged Care on the Exposure Draft Healthcare Identifiers Amendment (Consumer Access) Regulations 2023
- providing advice to the Department of Health and Aged Care about the potential privacy risks of the HI Framework Project
- responding to members of the community who had raised concerns about the unauthorised collection of their IHI included on a COVID-19 digital vaccination certificate.

Guidance

The OAIC updated privacy guidance regarding IHIs on COVID-19 digital vaccination certificates in December 2022. The guidance relates to the collection of COVID-19 digital vaccination certificates which contain an IHI and was updated to reflect the removal of IHIs from vaccination certificates from 3 December 2022 onwards.

Media enquiries

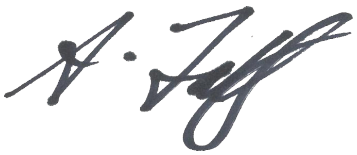
There were no media enquiries for the OAIC about the HI Service in 2022–23.

Other activities

Monitoring developments in digital health and the Healthcare Identifiers Service

The OAIC monitors developments in digital health to ensure the OAIC is positioned to offer informed advice about privacy aspects of the HI Service in the broader digital health context. During the reporting period the OAIC:

- monitored developments relating to digital health and the HI Service through news and digital health websites
- as outlined above in relation to the My Health Record system, attended various forums and conferences related to digital health which considered the HI Service in the broader digital health context.



Angelene Falk

Australian Information Commissioner and Privacy Commissioner

26 September 2023

Australian Government

Office of the Australian Information Commissioner

Annual Report of the Australian Information Commissioner's activities in relation to digital health 2022–23

oaic.gov.au

corporate@oaic.gov.au

OAIC