Annual Report of the Australian Information Commissioner's activities in relation to digital health 2024–25

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

Please attribute the content of this publication as:

Office of the Australian Information Commissioner, *Annual Report of the Australian Information Commissioner's activities in relation to digital health 2024–25*.

Contact

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

Online: guidanceandpublications@oaic.gov.au
Website: oaic.gov.au
Phone: 1300 363 992

Mail: Director, Guidance and Publications
Office of the Australian Information Commissioner
GPO Box 5218
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.

Contents

Acknowledgment of Country

We acknowledge the traditional custodians of Australia and their continuing connection to land, sea and community. We pay our respects to the people, the cultures and the elders past, present and emerging.

Executive summary

This annual report sets out the Australian Information Commissioner's digital health compliance and regulatory activity during 2024–25, 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).

Whether it's the use of Artificial Intelligence (AI) to record doctor-patient consultations, the availability of remote patient monitoring via telehealth, or the increasing use of wearable devices by patients, innovations in the realm of digital healthcare have continued to develop in 2024–25, enhancing opportunities to improve patient outcomes and the healthcare system more broadly.

These exciting innovations in healthcare delivery all have one thing in common: they have privacy and information governance impacts that require careful consideration. Regard must be given to how novel healthcare solutions can be supported and strengthened to realise health benefits while protecting Australians' most sensitive information, with a focus on privacy by design.

The Australian Government administers two key systems that underpin digital health in Australia: the Healthcare Identifiers Service (HI Service), and the My Health Record system. The legislation establishing the My Health Record system and HI Service include important privacy provisions, which recognise the special sensitivity of health information, and protect and restrict its collection, use and disclosure.

The Office of the Australian Information Commissioner (OAIC) is the independent privacy regulator for both systems, and our privacy oversight of these two systems is the focus of this annual report. Both systems involve the management of personal information. For the purposes of this report, we refer to them collectively as 'digital health'.

This report provides statistics about digital health activities undertaken by the OAIC during 2024–25, including complaints received by the Commissioner in relation to the My Health Record system, investigations made by the Commissioner in relation to My Health Records or the My Health Record system, enforceable undertakings accepted by the Commissioner under the My Health Records Act, and proceedings taken by the Commissioner in relation to civil penalty provisions, enforceable undertakings or injunctions.

This report also provides information about the Information Commissioner's compliance and enforcement activities under the Health Identifiers Act.

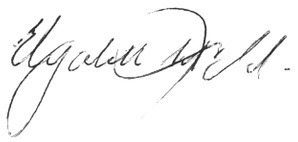
While full statistics are set out in the body of this report, the overall number of new digital health privacy complaints we received in 2024–25 has decreased. In 2024–25, the OAIC received 3 privacy complaints relating to the My Health Record system, compared with 15[1] in the previous year (a drop of 80%). We did not receive any privacy complaints relating to the HI Service in 2024–25, which is a reduction from 1 complaint in the previous year.

This report also includes information about notifiable data breaches related to digital health. In 2024–25 we received 18 data breach notifications in relation to the My Health Record system. This compares with 39 data breach notifications in relation to the My Health Record system in the previous year, amounting to a 54% decrease.

[1] This was recorded as 13 complaints in the 2023–24 Digital Health Annual Report, however that figure has been revised to 15 due to reclassification of matters.

To support the effectiveness of our digital health regulatory oversight, the OAIC has continued to contribute to policy measures relating to digital health and privacy in 2024–25, including:

- providing advice to stakeholders, including the Australian Digital Health Agency (ADHA), Services Australia and the Department of Health, Disability and Ageing about privacy-related matters relevant to the My Health Record system and HI Service, including:
    - the Department of Health, Disability and Ageing's review of the My Health Records legislative instruments and Healthcare Identifiers Regulations 2020 (HI Regulations)
    - the Department of Health, Disability and Ageing's framework for the use of My Health Record data for research and public health purposes
    - the ADHA's guidance for Pathology and Diagnostic Imaging providers relating to obligations under rule 42 of the My Health Records Rule 2016
- engaging with stakeholders such as the Australian Health Practitioner Regulation Agency, the Australian Commission on Safety and Quality in Health Care, Therapeutic Goods Administration, Australian Digital Health Agency and the Royal Australian College of General Practitioners about developments in health technologies that may impact on digital health and privacy, such as AI scribes
- developing and promoting guidance materials:
    - updating Chapter 8 of the OAIC Guide to Health Privacy to clarify clinicians' discretion to assist patients with notifying their at-risk relatives about genetic risk information without breaching federal privacy laws, and
- monitoring developments in the My Health Record system and the HI Service.



Elizabeth Tydd
Information Commissioner
25 September 2025

Carly Kind
Privacy Commissioner
25 September 2025

Part 1 Overview

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 OAIC 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 2024–25, the OAIC's regulatory oversight of the My Health Record system included:

- responding to enquiries
- investigating and resolving complaints
- handling data breach notifications
- providing privacy advice
- conducting privacy assessments and investigations, and
- contributing to policy development through stakeholder engagement.

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 2024–25 financial year.

Table 1: OAIC My Health Record and HI Service activities 2024–25

Activity	My Health Record	HI Service
Telephone enquiries	11	1
Written enquiries	7	0
Complaints received	3	0
Complaints[2] finalised	16	1
Commissioner-investigated investigations finalised	0	0
Assessments completed or in progress	2	0
Enforceable undertakings accepted	0	0
Proceedings taken in relation to civil penalty provisions, enforceable undertakings or injunctions	0	0
Data breach notifications received	18	N/A[3]
Data breach notifications finalised	18	N/A[3]

[2] A complaint may cover more than one issue.
[3] N/A is listed for data breach notifications for the HI Service because there are no mandatory data breach reporting requirements under the Healthcare Identifiers 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 about privacy aspects of the My Health Record system, including through preliminary inquiries, conciliation, investigation or deciding against investigating a complaint
- investigate, on the Commissioner's own initiative, acts and practices that may contravene 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 impacted entities to manage data breaches in accordance with the My Health Record legislative requirements
- investigate failures to notify eligible data breaches
- exercise a range of enforcement powers in relation to contraventions of the My Health Record 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 My Health Record system to ensure their compliance with privacy obligations
- develop statutory and regulatory guidance for consumers and other My Health Record system participants, such as healthcare providers, registered repository operators and the Australian Digital Health Agency (ADHA)
- maintain guidance for exercising the powers available to the Commissioner regarding the My Health Record system.

We also respond to enquiries and requests for regulatory policy advice from stakeholders about the My Health Record system's privacy framework and the appropriate management 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 professional industry bodies in the health sector in the course of undertaking our My Health Record activities, such as handling privacy-related enquiries and developing regulatory advice. Information about the OAIC's compliance and regulatory activities is provided below.

OAIC compliance and regulatory activities

Complaints and investigations relating to the My Health Record system

The OAIC received 3 complaints about the My Health Record system during 2024–25, which is a decrease of 80% on the previous financial year (where we received 15 complaints). We finalised 1 of those 3 complaints, in addition to finalising 9 complaints we received in 2023–24, 2 complaints we received in 2022–23, and 4 complaints we received in 2021–22.

As of 30 June 2025, the OAIC has not opened investigations into any complaints received from individuals about the My Health Record system during the reporting period.

The OAIC made no determinations under the *Privacy Act* during 2024–25 in relation to compliance with the My Health Records Act. [4]

Assessments relating to the My Health Record system

In 2024–25, the OAIC commenced 2 assessments of private hospitals, examining their preparedness to respond to data breaches in the MHR system. The OAIC also finalised our assessment of the ADHA's *myhealth* mobile health application.

-80%
Decrease in complaints

Table 2: Assessments relating to the My Health Record system

Assessment subject	Number of entities assessed	Year opened	Status
Mobile health application	1	2023–24	Complete
Private hospital preparedness to respond to data breaches in the MHR system [5]	1	2024–25	Ongoing
Private hospital preparedness to respond to data breaches in the MHR system [5]	1	2024–25	Ongoing

[4] This percentage is based on there being 15 My Health Record complaints in 2023–24.
[5] Two separate entities are being assessed.

Assessment snapshot

Assessment of a mobile health application

The OAIC assessed the Australian Digital Health Agency's *myhealth* mobile health application and its compliance with APPs 1.2 (open and transparent management of personal information), APPs 1.3 and 1.4 (clearly expressed and up-to-date APP Privacy Policy about how the entity manages personal information) and APP 5 (notification of the collection of personal information).

The assessment identified 3 medium privacy risks regarding the *myhealth* app's privacy policy's compliance with APPs 1.3 and 1.4.

We completed this assessment in 2024 and it is available on our website at Handling of personal information: my health app | OAIC. The assessment made 3 recommendations, namely that the ADHA should:

1. provide greater clarity around overseas disclosure of personal information, and ensure that information about these disclosures in the policy reflects current practice
2. update the language used in the *myhealth* app privacy policy to ensure users can consistently differentiate between the *myhealth* app and the user's My Health Record and, at point 2.0 in the *myhealth* app privacy policy, change the word 'collect' to the words 'permanently store', and
3. review the *myhealth* app privacy policy to consider the relevance of the content included in the policy to the management of personal information.

Enforceable undertakings

The Commissioner has not requested any enforceable undertakings in relation to My Health Record compliance action in 2024–25 or in previous years.

Proceedings taken in relation to civil penalty provisions, enforceable undertakings or injunctions

The Commissioner has not taken any proceedings in relation to civil penalty provisions, enforceable undertakings or injunctions in relation to My Health Record compliance action in 2024–25 or in previous years.

Data breach notifications

In 2024–25, the OAIC received 18 data breach notifications in relation to the My Health Record system and closed 18 notifications.

18 **Data breach notifications**

Table 3: Data breach notifications 2024–25

	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**
Australian Digital Health Agency	0	0	0	0	0	0
Services Australia	0	0	0	0	0	0
Health care provider organisations	18	128	128	18	128	128
Total*	18	128	128	18	128	128

*Totals across agencies may not match due to different reporting obligations

My Health Record system enquiries and guidance

Enquiries

My Health Record system enquiries

The OAIC's enquiries team received 11 telephone enquiries and 7 written enquiries about the My Health Record system during the 2024–25 reporting period.

Guidance

For health service providers

In 2024–25, the OAIC updated Chapter 8 of the *Guide to Health Privacy*, to assist clinicians to better understand their obligations under the Privacy Act when notifying at-risk relatives of genetic information with patient consent.

The updates to Chapter 8 clarify that clinicians may legally collect relatives' contact details from patients and use those to contact at-risk relatives where there is patient consent. The updates make no changes to the current guidance about notification without patient consent.

The guidance makes it clear that the collection and use of the relative's contact details must still be done in accordance with the Privacy Act, but is permitted where a clinician reasonably believes the collection and use are necessary to lessen or prevent a serious threat to the life, health or safety of that relative.

The Privacy Act requires that certain types of personal information are only collected or used with the consent of the person to whom the personal information belongs, unless it is unreasonable or impracticable to obtain consent (s16A (1)). The updated Chapter 8 guidance clarifies it is likely to be impracticable to seek a relative's prior consent to collection or use of their contact details, as the health professional will not know about the relative other than through the patient and cannot contact the relative without collecting the contact details from the patient.

The updated guidance clarifies health providers' key obligations when collecting, using and disclosing information in the case of a serious threat, both with and without the consent of the patient.

As outlined in the updated chapter, depending on the context, both sections 16B(4) and 16A of the Privacy Act may apply to permit the handling of personal information in a health situation without consent.

It is likely to be impracticable to seek a relative's prior consent to collection and use of their contact details, as the health professional will not know about the relative other than through the patient, and cannot contact the relative without collecting the contact details from the patient.

'Cascade' genetic testing (identifying relatives of affected individuals who may be at increased genetic risk) is an important mechanism for identifying and providing access to preventative care for at-risk individuals, improving public health generally. Cascade contact of at-risk relatives, where consent is given, can occur when each genetic relative (who is notified about their increased risk and makes contact with the disclosing health practitioner) is asked for consent to contact his or her genetic relatives. When additional genetic relatives make contact, the process is repeated. This process can provide access to genetic information for a wider cross-section of the family. However, in some cases consent may not be given.

The guidance makes it clear that it is not intended to imply the existence of an obligation for health service providers to identify and contact all relatives who may be at high risk of having a genetic predisposition, and clarifies how the Privacy Act applies to providers who choose to do so.

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 of how to make a complaint.

Liaison

Liaison with the Australian Digital Health Agency

The OAIC has continued liaising with the ADHA as required during the reporting period, 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 our regulatory role.

During the reporting period OAIC staff met with various health focused agencies and regulatory bodies to discuss the uptake in AI scribes across the medical profession, including the Australian Health Practitioner Regulation Agency, the Australian Commission on Safety and Quality in Health Care (ACSQHC), Therapeutic Goods Administration, Australian Digital Health Agency and the Royal Australian College of General Practitioners. We reviewed AI guidance developed by ACSQHC and provided comments relating to privacy impacts. OAIC staff also met with AI Scribe providers to better understand potential privacy impacts resulting from use in a clinical setting.

Part 3
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 HI Regulations.

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 to 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 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.