Australian Government

Office of the Australian Information Commissioner

Annual Report of the Australian Information Commissioner's activities in relation to digital health 2021–22

OAIC

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 2021–22*.

Contact

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

Online: oaic.gov.au/enquiry
Website: oaic.gov.au
Phone: 1300 363 992

Mail: Director, Strategic Communications
Office of the Australian Information Commissioner
GPO Box 5218
Sydney NSW 2001

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

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.

Contents

Executive summary

This annual report sets out the Australian Information Commissioner's (Information Commissioner) digital health compliance and enforcement activity during 2021–22, in accordance with s 106 of the *My Health Records Act 2012* and s 30 of the *Healthcare Identifiers Act 2010* (HI Act).

The report provides information about digital health activities led by the Office of the Australian Information Commissioner (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.

This was the 10th year of operation of the My Health Record system and the 12th year of the Healthcare Identifiers Service (HI Service), a critical enabler for the My Health Record system and digital health generally.

The management of personal information is at the core of both the My Health Record system and the HI Service (which are collectively referred to as 'digital health' in this report). In recognition of the special sensitivity of health information, the My Health Records Act and the HI Act contain provisions that protect and restrict the collection, use and disclosure of personal information. The Information Commissioner oversees compliance with those privacy provisions.

The My Health Record system commenced in 2012 as an opt-in system where an individual needed to register in order to get and share their My Health 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.

In 2021–22, the OAIC received 14 privacy complaints relating to the My Health Record system with 10 remaining open at the end of the reporting period. We finalised 5 My Health Record system complaints, including 1 complaint from previous reporting periods.

We received 11 privacy complaints relating to the HI Service in 2021–22. We finalised 1 of those complaints received in 2021–22. There were no HI Service complaints from the previous reporting period.

Over the reporting period, there was a marked increase in the OAIC's policy work in relation to the HI Service as well as an increase in complaints and enquiries about healthcare identifiers. This increase is primarily attributed to the inclusion of healthcare identifiers on COVID-19 vaccine certificates and the subsequent increased collection and overall visibility of healthcare identifiers. To help ensure compliance with the HI Act and encourage best privacy practice in relation to the handling of healthcare identifiers, the OAIC published privacy guidance to assist entities and individuals that collect a person's COVID-19 digital vaccination certificate which contains an Individual Healthcare Identifier (IHI).

We received 3 data breach notifications during the reporting period in relation to the My Health Record system and closed 3 notifications.

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

- commencing one privacy assessment and progressing another assessment commenced in the previous reporting period
- providing advice to stakeholders, including the Australian Digital Health Agency (ADHA), Services Australia and the Department of Health and Aged Care, on privacy-related matters relevant to the My Health Record system and HI Service
- developing and promoting guidance materials, including publishing new resources about IHIs and developing and conducting consultation on guidance and a new template for healthcare providers to help them comply with security and access policy requirements under the My Health Records Rule 2016
- presenting a webinar to healthcare providers on the OAIC's Privacy and My Health Record assessments and providing panel members for a Q&A session, and
- monitoring developments in digital health, 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 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 2021–22, 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
- promoting existing guidance about the My Health Record emergency access function and developing new guidance and 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 a digital health podcast to support and promote the OAIC's My Health Record emergency access resources
- publishing privacy guidance regarding IHIs on COVID-19 digital vaccination certificates
- raising risks associated with the registration requirements of healthcare providers in the My Health Record system with the service operator and AHDA
- presenting a webinar to healthcare providers on the OAIC's Privacy and My Health Record assessments and conducting a panel Q&A session, and
- engaging with the ADHA about the performance audit the Australian National Audit Office (ANAO) conducted of the My Health Record system and the ADHA's implementation of the ANAO's recommendations, as well as privacy aspects of the system more generally.

Funding

Prior to 1 July, 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 undertaken by the OAIC during the 2021–22 financial year.

Table 1: OAIC My Health Record and HI Service activities 2021–22

Activity	My Health Record	HI Service
Telephone enquiries	15	15
Written enquiries	9	11
Complaints received	14	11
Complaints finalised	5	1
Commissioner-investigated investigations finalised	0	0
Policy advices	36	20
Assessments completed or in progress	2	0
Data breach notifications received	3	0
Data breach notifications finalised	3	0
Media enquiries	0	2

* A complaint may cover more than one issue.

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 enforcement activities 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 as the Commissioner considers appropriate, 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 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 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 enforcement and compliance activities

Complaints and investigations relating to the My Health Record system

The OAIC received 14 complaints about the My Health Record system during 2021-22, 4 of which were finalised. We also finalised one complaint about the My Health Record system from 2020-21.

The Commissioner did not initiate any investigations related to the My Health Record system during the reporting period.

Assessments relating to the My Health Record system

In the 2021–22, the OAIC conducted 2 My Health Record privacy assessments as part of the My Health Record access security policy assessment program. Both assessments will be finalised in 2022–23.

Table 2: Assessments relating to the My Health Record system conducted in 2021-22

Assessment subject	Number of entities assessed	Year opened	Status[1]
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	Ongoing
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	Ongoing

Assessment snapshots

My Health Records Assessment 1

The first My Health Record assessment commenced in the 2020–21 financial year. 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.

The OAIC conducted this assessment under Australian Privacy Principle (APP) 11.1, given that compliance with Rule 42 is a reasonable step the OAIC would expect health service providers to take when securing the personal information they collect and hold.

The OAIC will finalise this assessment early in the 2022-23 financial year and prepare a de-identified assessment report which provides demographic information about the sample assessed and aggregated findings.

[1] Status shown is as at 30 June 2022. Both assessments will be finalised in the 2022-23 financial year.

My Health Records Assessment 2

In the 2021–22 financial year, the OAIC assessed 20 GP clinics across Australia (selected out of the 300 GP clinics in Assessment 1). The OAIC examined the 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.

The assessment involved a review of the GP clinics' Security and Access policies and interviews with representatives from each GP clinic.

The OAIC will finalise this assessment early in the 2022-23 financial year and prepare a de-identified assessment report which provides aggregated findings as well as recommendations and suggestions for each assessed GP clinic in relation to identified privacy risks.

Data breach notifications

In 2021–22, the OAIC received 3 data breach notifications during the reporting period in relation to the My Health Record system and closed 3 notifications.

Table 3: Data breach notifications 2021–22

	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	4	4	1	4	4
Services Australia	0	0	0	0	0	0
Healthcare provider organisations	2	2	2	2	2	2

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

Advice

My Health Record system enquiries

The OAIC's enquiries team received 15 telephone enquiries and 9 written enquiries about the My Health Record system during the reporting period.

Policy advice to stakeholders

During the reporting period, the OAIC provided 36 pieces of policy advice to various stakeholders related to the My Health Record system. These included:

- providing feedback to the Australian Commission on Safety and Quality in Health Care (ACSQHC) on their privacy fact sheet for digital mental health service providers, including their obligations under My Health Records legislation. The OAIC also met with the ACSQHC to discuss further resources and education initiatives
- raising awareness of vulnerabilities in the system associated with the registration process for healthcare providers in the My Health Record system with the service operator and AHDA
- providing advice to the Department of Health in relation to the implementation of recommendations made as part of the My Health Records Legislative Review, conducted by Professor John McMillan AO
- providing advice to a healthcare provider about the requirements for practice managers to access the My Health Record system.

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:

- working in collaboration with the ADHA to develop a security and access policy template to assist healthcare provider organisations in meeting the requirements set out in Rule 42 of the My Health Records Rule 2016. Two consultation sessions with external stakeholders were undertaken to seek feedback on the template prior to its publication
- assisting in the development and participating in the recording of a My Health Record emergency access podcast to guide the appropriate use of the emergency access function
- reviewing and providing feedback on the ADHA's My Health Record digital wallet APP 5 notices and declarations.

Guidance

For health service providers

The OAIC's guidance focus in 2021-22 was the development of a security and access policy template to help healthcare providers comply with their obligations under Rule 42 of the My Health Records Rule 2016 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 will be available for download as a customisable Word document. The template was informed by the OAIC's assessments on Rule 42

compliance and stakeholder feedback received through an extensive consultation with clinical peak bodies, primary health networks and ADHA clinical leads.

The template will be 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 on the ADHA's new eLearning course to further assist users of the template.

The OAIC's security and access policy template and new guidance will be published and available for download in early 2022-23.

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 making 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 and the My Health Record system to inform its regulatory role. During the reporting period, staff attended:

- the annual Digital Health Institute Summit on 21-22 February 2022. The conference was organised by Australasian Institute of Digital Health (AIDH) and focused on healthcare strategies in a digital world
- the ADHA webinar: "What Australians have told us they want for the next National Digital Health Strategy". The focus of the webinar was to inform participants about what Australians want for the future of digital health, based on the National Digital Health Strategy survey
- the Department of Health's Data Strategy 2022 – 2025 Roundtable discussion. The Data Strategy and associated implementation roadmap are intended to drive strategic activities in the context of Departmental and portfolio-wide priorities and to respond to data and analytics developments across government more broadly.

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 HI Service is a foundation service for a range of digital health initiatives in Australia, particularly the My Health Record system. The use of healthcare identifiers has increased since the launch of the My Health Record system on 1 July 2012. 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.

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 as the Commissioner considers appropriate, 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 advice and guidance material.

OAIC compliance and enforcement activities

Complaints relating to the Healthcare Identifiers Service

The OAIC received 11 complaints about healthcare identifiers in 2021-22, 1 of which was finalised in the reporting period.

Investigations relating to the Healthcare Identifiers Service

No complaint investigations or Commissioner-initiated investigations were commenced or finalised during the reporting period. As of 30 June 2022, 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 2021–22.

HI Service advice, guidance, liaison and other activities

Advice

HI Service enquiries

The OAIC's enquiries team received 15 phone enquiries, and 11 written enquiries about the handling of healthcare identifiers during the reporting period.

Policy advice to stakeholders

In relation to the HI Service, the OAIC provided 20 pieces of policy advice to stakeholders during the reporting period. This represents a significant increase in policy work compared to previous years. This increase is primarily due to the inclusion of IHIs on COVID-19 digital vaccination certificates and the subsequent risk of increased collection, use, disclosure and overall visibility of healthcare identifiers. Some examples of advice provided in relation to the HI Service include:

- providing advice to Services Australia about the application of the HI Act and privacy risks associated with the inclusion of IHIs on COVID-19 digital vaccination certificates
- responding to members of the community who had raised concerns about the inclusion of IHIs on COVID-19 digital vaccination certificates.

Guidance

The OAIC published privacy guidance regarding IHIs on COVID-19 digital vaccination certificates on 3 March 2022. The guidance is designed for any entity or individual that collects a COVID-19 digital vaccination certificate which contains an IHI. It provides advice on steps to take to avoid collecting IHIs, removing or redacting them if they have been collected, or otherwise ensuring compliance with the requirements of the HI Act.

Media enquiries

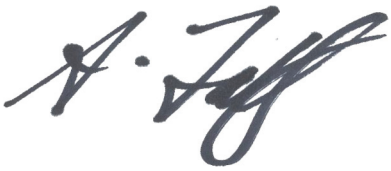
The OAIC responded to 2 media enquiries about the HI Service in 2021–22. Articles appeared in the Australian Financial Review and the West Australian newspaper concerning the implications of IHIs being included when employers collected or sighted vaccination certificates.

Other activities

Monitoring developments in digital health and the Healthcare Identifiers Service

The OAIC monitors developments in digital health and the HI Service 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, and 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

20 September 2022

Australian Government

Office of the Australian Information Commissioner

Office of the Australian Information Commissioner

1300 363 992

https://www.oaic.gov.au/about-us/contact-us

@OAICgov