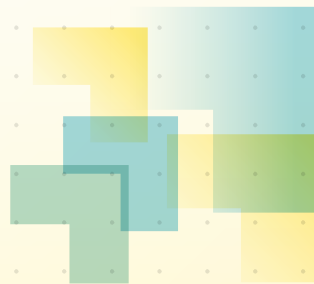
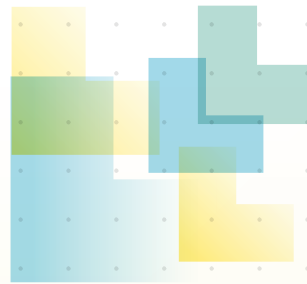




**Australian Government**  
**Office of the Australian  
Information Commissioner**

# Annual report of the Australian Information Commissioner's activities in relation to digital health 2020–21



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**

With the exception of the Commonwealth Coat of Arms, this Annual report of the Australian Information Commissioner's activities in relation to digital health 2020–21 is licensed under a Creative Commons Attribution 3.0 Australia licence ([creativecommons.org/licenses/by/3.0/au/deed.en](https://creativecommons.org/licenses/by/3.0/au/deed.en)).

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 2020–21.

### **Contact**

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

**Online:** [oaic.gov.au/enquiry](https://oaic.gov.au/enquiry)  
**Twitter:** @OAICgov  
**Website:** [oaic.gov.au](https://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**

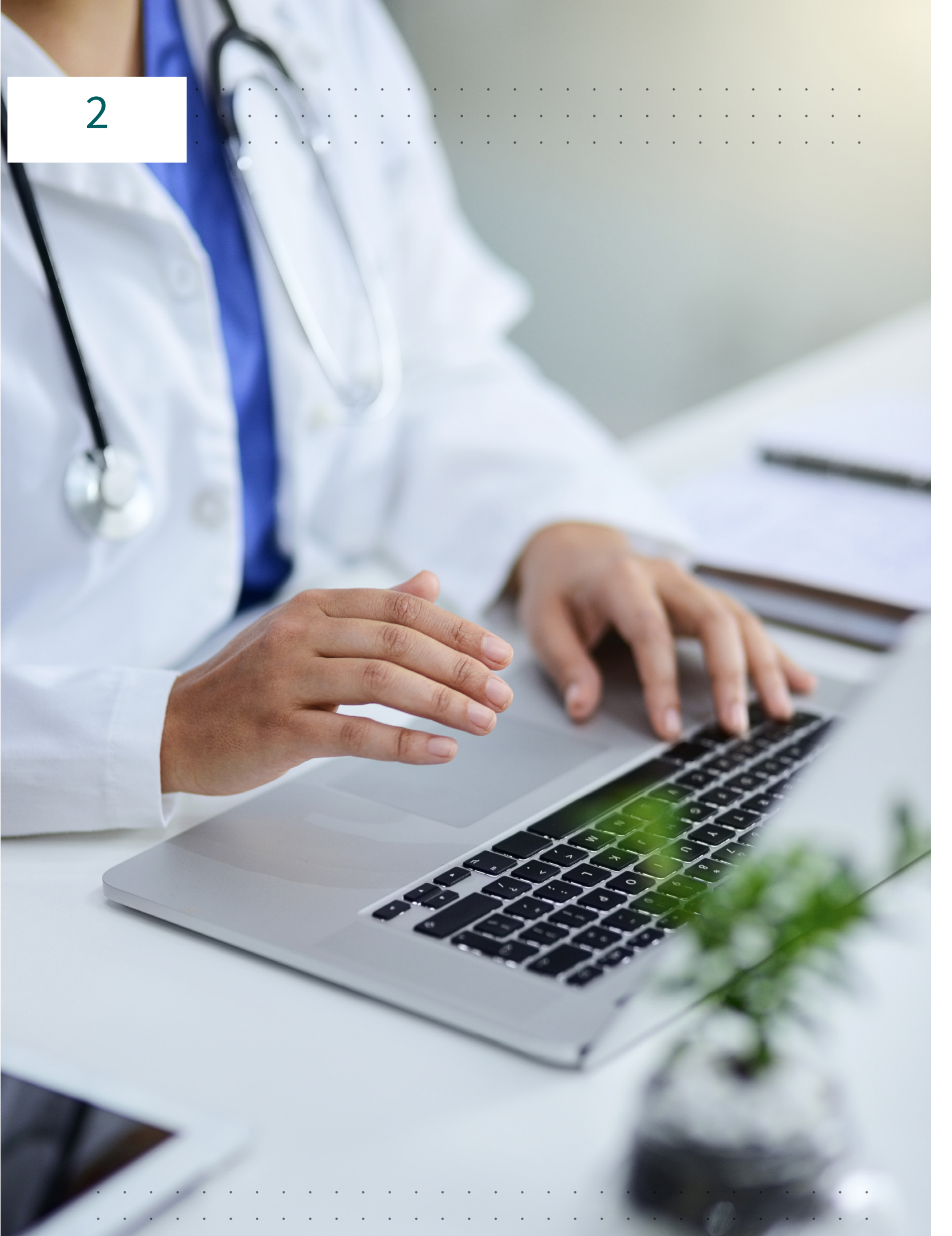
All our publications can be made available in a range of accessible formats. If you would like this report in an accessible format, please contact us.

### **Acknowledgement 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 ..... 3
- Part 1: Introduction ..... 4
  - Regulatory work of the OAIC..... 4
  - Memorandum of Understanding with the ADHA ..... 4
  - Year in review summary ..... 5
- Part 2: The OAIC and the My Health Record system..... 7
  - OAIC enforcement and compliance activities..... 7
  - Assessment snapshots ..... 9
  - My Health Record system advice, guidance, liaison and other activities..... 12
- Part 3: The OAIC and the Healthcare Identifiers Service ..... 15
  - OAIC compliance and enforcement activities ..... 15
  - HI Service advice, guidance, liaison and other activities ..... 16



## Executive summary

This annual report sets out the Australian Information Commissioner's (Information Commissioner) digital health compliance and enforcement activity during 2020–21, 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 other 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.

More information about the Memorandum of Understanding (MOU) between the OAIC and the Australian Digital Health Agency (ADHA) is provided in Part 1 of this report.

This was the ninth year of operation of the My Health Record system and the 11th 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 this report collectively refers to as 'digital health'). 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 2020–21, the OAIC received 7 privacy complaints relating to the My Health Record system with 3 remaining open at the end of the reporting period. We finalised 7 My Health Record system complaints, including 3 complaints from previous reporting periods.

We received one privacy complaint relating to the HI Service in 2020–21 which is ongoing. We finalised one HI Service complaint from the previous reporting period. No Commissioner-initiated investigations were opened during the reporting period. We closed one Commissioner-initiated investigation from the previous reporting period.

We received 3 data breach notifications during the reporting period in relation to the My Health Record system and closed 2 notifications with one ongoing. We also carried out digital health-related work including:

- commencing one privacy assessment and closing 3 privacy assessments
- providing advice to stakeholders, including the ADHA and the Department of Health, on privacy-related matters relevant to the My Health Record system
- developing and promoting guidance materials, including new resources about the My Health Record emergency access function and guidance for healthcare providers on Rule 42
- making a submission to the Department of Health on the review of the My Health Records Act
- 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* 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 our compliance and enforcement role, the OAIC performs proactive education and guidance functions. In 2020–21, 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
- 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
- engaging with the Department of Health on the review of the My Health Records Act, including making a written submission
- publishing new guidance about the My Health Record emergency access function and guidance for healthcare providers on Rule 42
- promoting existing guidance materials for health service providers, including the *Guide to health privacy*
- promoting consumer resources including information about privacy and the My Health Record system.

### Memorandum of Understanding with the ADHA

The 2020–21 MOU between the OAIC and the ADHA set out operational and funding arrangements between the parties and covered activities related to both the My Health Record system and the HI Service. It provided for a program of work that included business-as-usual activities (such as responding to requests for advice and investigating privacy complaints relating to digital health), and project-based work (such as developing guidance materials and conducting assessments). Information about these activities is set out in Parts 3 and 4 of this report. During the reporting period, the OAIC received \$2,070,000 (GST exclusive) under the MOU.

From 1 July 2021, the OAIC will receive a direct appropriation for our role as the independent privacy regulator for the My Health Record system and the HI Service and there will no longer be an MOU arrangement between the OAIC and the ADHA. The OAIC will continue to engage closely with the ADHA under the new arrangements to ensure the effective regulation of the digital health system and to ensure privacy is a key consideration in all initiatives.

## Year in review summary

The table below summarises the digital health activities undertaken by the OAIC during the 2020–21 financial year.

**Table 1: OAIC My Health Record and HI Service activities 2020–21**

Activity	My Health Record	HI Service
Telephone enquiries	9	1
Written enquiries	2	1
Complaints received	7*	1
Complaints finalised	7	1
Commissioner-initiated investigations (CIIs) finalised	1†	–
Policy advices‡	21	1
Assessments completed or in progress	4	–
Data breach notifications received	3	–
Data breach notifications finalised	2	–
Media enquiries	–	3

\* A complaint may cover more than one issue.

† This CII was opened in the previous reporting period.

‡ This includes submissions.





## Part 2: The OIAC and the My Health Record system

The OIAC 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 Information Commissioner considers appropriate, including through preliminary inquiries, conciliation, investigation or deciding not to investigate a complaint
- investigate, on the Information 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 Information 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 My Health Record 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 Information 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 OIAC's regulatory role under the My Health Record system.

The OIAC 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 OIAC's activities in relation to providing advice, developing guidance material and liaison with key stakeholders is provided below.

### OIAC enforcement and compliance activities

#### Complaints and investigations relating to the My Health Record system

The OIAC received 7 complaints about the My Health Record system during 2020–21, 4 of which were finalised. We finalised one complaint about the My Health Record system from 2019–20 and 2 complaints from 2018–19.

We did not open any new Commissioner-initiated investigations during the reporting period. We closed one Commissioner-initiated investigation from a previous reporting period.

## Assessments relating to the My Health Record system

Under the MOU with the ADHA, the OAIC is required to conduct a minimum of 2 assessments during the 2020–21 financial year in relation to the My Health Record system and the HI Service.

The OAIC finalised 2 assessments relating to the My Health Record system in 2020–21 that began in 2019–20 and finalised one assessment that began in 2018–19. We commenced one assessment that will be finalised in 2021–22.

**Table 2: Assessments relating to the My Health Record system conducted in 2020–21**

Assessment subject	Number of entities assessed	Year opened	Status
1. Assessment of pathology and diagnostic imaging services – Australian Privacy Principles (APPs) 1.2 and 11 and Rule 42 of the My Health Records Rule	8	2018–19	Closed (1)*
2. Assessment of Chamonix mobile health application that accesses My Health Records – APPs 1.2 and 5	1	2020–21	Closed
3. Assessment of Telstra mobile health application that accesses My Health Records – APPs 1.2 and 5	1	2020–21	Closed
4. Assessment of general practice clinics – APPs 1.2 and 11 and Rule 42 of the My Health Records Rule	300	2020–21	Ongoing

\* The assessment was finalised for 7 of the 8 entities in the 2019–20 financial year, with the assessment for the one remaining entity finalised in the 2020–21 year.

## Assessment snapshots

### Assessment of 8 pathology and diagnostic imaging services – access controls for the My Health Record system

In 2020–21, the OAIC finalised an assessment of 8 pathology and diagnostic imaging services and their access controls for the My Health Record system. The assessment was finalised for 7 of the 8 entities in the 2019–20 financial year, with the assessment for the remaining entity finalised in 2020–21.

The assessment involved a self-administered questionnaire and desktop review of documentation. It examined whether these services had appropriate governance and information security arrangements to manage access security risks in accordance with Rule 42 of the My Health Records Rule and Australian Privacy Principles (APPs) 1.2 and 11. Each of the pathology and diagnostic imaging services was individually advised about their assessment results.

The assessment provides examples of compliance, non-compliance or partial compliance by registered healthcare provider organisations and participants in the My Health Record system with the Privacy Act and APPs and the My Health Records Rule. A de-identified summary report combining the findings for the pharmacies assessment and the pathology and diagnostic imaging services assessment was published in September 2020. Across the pathology and diagnostic imaging services, we found that:

- 17 of the 22 assessment targets had implemented a My Health Record system access security policy at the time of the assessment
- all assessment targets with an access security policy outlined the process for authorising staff access in the policy, however the majority of policies failed to document the requirement under Rule 44(e) to immediately suspend or

deactivate user accounts after becoming aware a user account has been compromised, although in practice this was done within 24 hours

- access security policies addressed the training to be provided to staff who access the My Health Record system, and the majority of assessment targets provide training to their staff before they are given access to the system, but areas for improvement include:
  - provision of training to staff of 3 assessment targets
  - provision of refresher training to staff of 12 assessment targets
  - inclusion of content about legal obligations of staff and the consequences of breaches
  - maintenance of training registers by 9 of the assessment targets
- in relation to physical and information security measures, while most assessment targets reported good physical security measures, most did not meet the ADHA's recommended standard for passwords used to access the My Health Record system
- in relation to risk management and risk mitigation strategies, most assessment targets reported having a procedure in place for identifying and responding to My Health Record-related security and privacy risks; however, there were areas for improvement in relation to recording matters relevant to security breaches under APP 11, and only 9 assessment targets used audit logs to monitor staff with access to the My Health Record system.

The OAIC also published guidance for healthcare provider organisations with responsibilities and obligations under Rule 42.

## Assessments of mobile health apps

In 2019–20, the OAIC commenced 2 assessments of mobile health applications that access My Health Records to determine whether these applications are handling the personal information of registered healthcare recipients in accordance with their obligations under the Privacy Act.

The scope of the assessments considered the handling of personal information in relation to the My Health Record system by Chamonix and Telstra Health and their respective mobile applications Healthi and HealthNow. The assessments considered compliance with APP 1.2 (Open and transparent management of personal information) and APP 5 (Notification of the collection of personal information).

To undertake the privacy assessments, the OAIC reviewed relevant policies and procedures provided by Chamonix and Telstra Health and conducted virtual interviews with key staff members in September and October 2020.

### Chamonix Healthi app

Chamonix's Healthi app only provides 'read-only' access to a user's My Health Record and does not have any other functionality. The OAIC found that Chamonix took reasonable steps to document its information handling policies, practices and procedures, and to notify individuals of the collection of personal information. However, we identified medium-level privacy risks associated with the handling of personal information through the Healthi app.

The OAIC made 4 recommendations and some suggestions to address these privacy risks, including that Chamonix regularly evaluate its internal policies and procedures, implement regular and mandatory privacy refresher training, include an APP 5 collection notice in relation to personal information collected via the Healthi webform or via email, and ensure that the Healthi collection notice covers all APP 5 matters.

### Telstra Health HealthNow app

Telstra Health's HealthNow app provides a range of eHealth services to users, including the facilitation of 'view-only' access to a user's My Health Record.

The OAIC found that Telstra Health is taking reasonable steps to document and implement practices, procedures and systems to ensure they comply with the APPs, and to enable the effective handling of privacy enquiries and complaints in relation to the HealthNow app.

The assessment also found that Telstra Health is taking reasonable steps to notify HealthNow users of APP 5 matters, and ensure their understanding of APP 5 matters in relation to the collection of personal information by the app.

We made one recommendation that Telstra Health revise the HealthNow Privacy Statement and in-app notifications to delineate clearly between the collection, use and disclosure of My Health Record data, and the collection, use and disclosure of other types of personal information collected by the app.

## Assessment of general practice clinics – APPs 1.2 and 11 and Rule 42

In 2020–21, the OAIC commenced an assessment of 300 general practice (GP) clinics' compliance with the requirements of Rule 42 of the My Health Records Rule, which requires entities to have an access security policy. The assessment is being conducted under APP 11.1, given that compliance with Rule 42 is a reasonable step that the OAIC would expect health service providers to take when securing the personal information they collect and hold. The OAIC anticipates finalising this assessment during 2021–22 and publishing a de-identified assessment report which provides sector analysis and aggregated findings.

## Data breach notifications

In 2020–21, the OAIC closed 2 out of the 3 data breach notifications we received in relation to the My Health Record system. There is one ongoing data breach notification.

No data breach notifications were received from Services Australia during this reporting period.<sup>1</sup>

**Table 3: Data breach notifications 2020–21**

Notifying party	Notified in the period			Closed in the period		
	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	2	1	1	1	1	1
Private healthcare organisation	1	1	1	1	1	1
Services Australia	–	–	–	–	–	–

<sup>1</sup> The Chief Executive of Medicare (part of Services Australia) is a registered repository operator under s 38 of the My Health Records Act.

## 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 2 written enquiries about the My Health Record system during the reporting period.

#### Policy advice to stakeholders

During the reporting period, the OAIC provided 21 policy advices to various stakeholders related to the My Health Record system. These included:

- presentation to the ADHA's professional indemnity insurers workshop about My Health Record system assessments in September 2020
- engagement with the Department of Health regarding digital health work and future planning
- comments on National Safety and Quality Digital Mental Health Standards guide for service providers
- advice to the Consumers Health Forum of Australia in response to their query on the My Health Record emergency access function.

#### Policy advice to the ADHA

Under the 2020–21 MOU with 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:

- consultation with the ADHA in relation to the ANAO's performance audit of the My Health Record system and implementation of the ANAO's recommendations, including meetings to discuss the ADHA's draft Compliance Framework and its

application in the context of the My Health Record emergency access function

- advice regarding the ADHA's National Infrastructure Modernisation Program, which supports the National Digital Health Strategy
- advice regarding registration requirements for healthcare providers and other operational matters under the My Health Records Act
- advice regarding the Notifiable Data Breaches scheme under the Privacy Act
- participation in a briefing on the ADHA's operations and activities in June 2021.

### Guidance

#### For health service providers

The OAIC has continued to promote guidance materials and resources about the My Health Record system across a range of channels. In 2020–21 we published the following resources:

- Rule 42 Guidance (4 September 2020)
- My Health Record emergency access function guidance (June 2021)
- My Health Record emergency access function FAQs (June 2021)
- My Health Record emergency access function flowchart (June 2021).

#### 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.

The OAIC regularly promotes awareness of these consumer-facing privacy resources through our social media channels.

## Other external engagement

In 2020–21, the OAIC developed new My Health Record emergency access guidance for healthcare providers, in consultation with the ADHA. The OAIC engaged peak health bodies such the Australian Medical Association, Royal Australian College of General Practitioners and the Consumers Health Forum of Australia to understand the clinical applications of the emergency access function.

- Digital Health Festival (Digifest), Melbourne (June 2021)
- Australasian Institute of Digital Health HealthData21 conference (June 2021)
- Talking Tech: My Health Record, Sydney (June 2021).

## Liaison

### Liaison with the ADHA

The OAIC liaised regularly with the ADHA to discuss MOU activities and other matters relating to the My Health Record system as well as the ADHA's implementation of the ANAO's recommendations following its performance audit of the My Health Record system.

### Liaison with other key stakeholders

The OAIC held 2 meetings with the Department of Health to discuss their response to the review of the My Health Records legislation and other digital health projects.

## Other activities

### Monitoring developments in digital health and the My Health Record system

Under the MOU with the ADHA, the OAIC monitors developments in digital health and the My Health Record system to ensure it is able to provide informed advice about privacy aspects of the operation of the system and the broader digital health context. During the reporting period, staff attended:

- Australasian Institute of Digital Health (AIDH) Digital Health Institute Summit 2020 (November 2020)

## Review of My Health Records Act submission

The OAIC made a submission to the Department of Health on the review of the My Health Records Act. Led by Professor John McMillan AO, the review sought to ensure the legislation underpinning the My Health Record system is effective. The OAIC considered the review to be an important evaluative measure and an opportunity to ensure that the privacy and security of health information continues to be a central focus of the design and functionality of the My Health Record system. In our submission we:

- welcomed the development of a 'futures roadmap' or strategic plan for the My Health Record system as a way for stakeholders, including the OAIC, to understand how the system is intended to operate going forward
- noted that the ADHA is required by the Privacy (Australian Government Agencies – Governance) APP Code 2017 to undertake a privacy impact assessment for any high privacy risk projects
- observed that weakening the prohibited purposes provisions (employers and insurers) could impact the privacy of healthcare recipients and public confidence in the system, leading to possible reduced participation
- welcomed further consideration of the issues related to the existing framework for the handling of the health information of minors
- found that the existing provisions that establish the emergency access function appropriately balance privacy and clinical needs.

The OAIC recommended that:

- consideration be given to legislative amendments which would ensure the application of the Information Commissioner's role in assessing, investigating and enforcing the My Health Records Act fully extends to all participants in the system
- a mechanism for external oversight of healthcare provider registration be established
- the permitted disclosure regime be expanded to allow disclosures of certain risks identified through the OAIC's regulation of the My Health Record system to the ADHA
- the My Health Record Rule deals with the status of a person's My Health Record upon death and that the necessity and proportionality of the requirement to retain records 30 years after death (or for 130 years if the date of death is not known) be reconsidered
- the existing My Health Record data breaches scheme, which captures a broader range of data breaches compared to the Notifiable Data Breaches scheme under the Privacy Act, be retained
- s 44 and s 51(3) of the My Health Records Act be amended to introduce positive obligations on the ADHA in relation to the registration of healthcare providers.





## 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 Information Commissioner considers appropriate, including through preliminary inquiries, conciliation, investigation or deciding not to investigate a complaint
- investigate, on the Information 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 HI Service

The OAIC received one complaint about healthcare identifiers in 2020–21 and finalised one complaint received in an earlier reporting period.

#### Investigations relating to the HI Service

No complaint investigations or Commissioner-initiated investigations were commenced or finalised during the reporting period. As at 30 June 2021, there were no HI Service investigations open.

#### Assessments relating to the HI Service

The OAIC did not initiate any assessments of the HI Service in 2020–21. We have been conducting follow-up on the assessment of Healthscope Group's information security controls to protect Individual Healthcare Identifiers which was closed in the 2019–20 reporting period.

## HI Service advice, guidance, liaison and other activities

### Advice

#### HI Service enquiries

The OAIC’s Enquiries team received one telephone enquiry and one written enquiry about the HI Service during the reporting period.

#### Policy advice to stakeholders

In relation to the HI Service, the OAIC received one request for advice from the ADHA about Individual Healthcare Identifiers.

### Guidance

#### Media enquiries

The OAIC responded to 3 media enquiries about the HI Service in 2020–21.

#### Angelene Falk

Australian Information Commissioner and Privacy Commissioner

20 September 2021

### Other activities

#### Monitoring developments in digital health and the Healthcare Identifiers Service

Under the 2020–21 MOU with the ADHA, the OAIC is required to monitor developments in digital health and the HI Service to ensure the OAIC is aware of the implications of any developments for the HI Service and is able 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 clips 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.





**Australian Government**  
**Office of the Australian  
Information Commissioner**



Annual report of the Australian Information Commissioner’s activities  
in relation to digital health 2020–21

1300 363 992  
Online: [oaic.gov.au/enquiry](https://www.oaic.gov.au/enquiry)  
@OAICgov

