Australian Government

Office of the Australian Information Commissioner

Annual Report of the Australian Information Commissioner's activities in relation to digital health 2019–20

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

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 2019–20.

Contact

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

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

Email: enquiries@oaic.gov.au

Website: www.oaic.gov.au

Phone: 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

2

Part 1: Executive summary

This annual report sets out the Australian Information Commissioner's digital health compliance and enforcement activity during 2019–20, in accordance with s 106 of the *My Health Records Act 2012* (My Health Records Act) and s 30 of the *Healthcare Identifiers Act 2010* (HI Act).

This report provides information about the OAIC's digital health activities, including its 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 eighth year of operation of the My Health Record system and the tenth 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 Australian 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 every Australian who had not opted out of the system.

In 2019–20, the OAIC received 10 privacy complaints relating to the My Health Record system with 1 remaining open at the end of the reporting period. We also finalised 19 complaints from the previous reporting period.

Three privacy complaints were received relating to the HI Service in 2019–20 with 1 remaining open at the end of the reporting period.

Six Commissioner-initiated investigations were opened during the reporting period, 5 of which were finalised with 1 remaining open at the end of the period.

The OAIC received 1 data breach notification in relation to the My Health Record system during 2019–20. This matter was closed at the end of the reporting period.

We also carried out digital health-related work including:

- commencing 1 privacy assessment, closing 4 privacy assessments and progressing 1 assessment from the reporting period
- providing advice to stakeholders, including the ADHA and the Department of Health, on privacy-related matters relevant to the My Health Record system
- updating and promoting guidance materials including the OAIC's *Guide to health privacy*
- monitoring developments in digital health, the My Health Record system and the HI Service.

Part 2: 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'.

The 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.

During the 2019–20 reporting period 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 investigations and assessments
- engaging with the ADHA about the Australian National Audit Office's (ANAO) performance audit 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
- promoting guidance materials, including the *Guide to health privacy*, a privacy action plan for health practices, and a new data breach action plan for health service providers
- promoting consumer resources including information about privacy and the My Health Record system.

Memorandum of Understanding with the ADHA

The MOU between the OAIC and ADHA sets out operational and funding arrangements between the parties relating to the MHR system and HI Service. The 2019–20 MOU came into effect on 1 July 2019 and during the reporting period, the OAIC received $2,070,000 (GST exclusive) under the MOU.

Information Commissioner's digital health functions

The My Health Record system

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
- provide a range of advice and guidance material
- maintain guidance for exercising the powers available to the Commissioner in relation to the My Health Record system.

Healthcare Identifiers Service

The Australian 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.

Year in review summary

Table 1: OAIC My Health Record and HI Service activities 2019–20

Activity	My Health Record	HI Service
Telephone enquiries	6	2
Written enquiries	1	–
Complaints received	10*	3
Complaints finalised	28	5
Commissioner-investigated investigations finalised or in progress	6	–
Policy advices	20	2
Assessments completed or in progress	5	1
Data breach notifications received	1	–
Media enquiries	3	–

* A complaint may cover more than one issue.

Part 3: 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.

Compliance and enforcement activities include:

- receiving, conciliating and investigating complaints about alleged interferences with the privacy of a healthcare recipient in relation to the My Health Record system
- conducting Commissioner-initiated investigations of any act or practice that may be a contravention of the My Health Records Act
- conducting assessments of participants in the system to ensure they are complying with their privacy obligations
- receiving data breach notifications from system participants.

The OAIC is also responsible for producing statutory and regulatory guidance for consumers and other participants such as healthcare providers, registered repository operators and the System Operator (the ADHA). In addition, the OAIC responds 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.

To deliver these outcomes, the OAIC liaised with external stakeholders, including professional industry bodies in the health sector. 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 10 complaints about the My Health Record system during 2019–20, 9 of which were finalised. Nineteen complaints about the My Health Record system from the previous reporting period were finalised during 2019–20. Six Commissioner-initiated investigations were opened during the reporting period, 5 of which were finalised with 1 remaining open at the end of the period.

Assessments relating to the My Health Record system

The OAIC commenced 1 assessment relating to the My Health Record system in 2019–20 and progressed 1 assessment that began in 2018–19. We closed 2 assessments that began in 2018–19 and 1 assessment that began in 2017–18.

Table 2: Assessments relating to the My Health Record system conducted in 2019–20

Assessment subject	Number of entities assessed	Year opened	Closed
1. Assessment of the ADHA — reasonable steps to protect personal information held in the My Health Record system — Australian Privacy Principle (APP) 11 and the My Health Record Act	1	2017–18	Closed
2. Assessment of private hospitals — access controls for the My Health Record system — APPs 1.2 and 11, and Rule 42 of the My Health Record Rules	2	2018–19	Closed
3. Assessment of pharmacies — access controls for the My Health Record system — Rule 42 of the My Health Record Rules	14	2018–19	Closed
4. Assessment of pathology and diagnostic imaging services — APPs 1.2 and 11, and Rule 42 of the My Health Record Rules	8	2018–19	Ongoing*
5. APPs 1.2 and 5 assessment of mobile health applications that access My Health Records	2	2019–20	Ongoing

* The assessment of one of the 8 entities remains ongoing.

Assessment snapshots

Assessment of the ADHA — reasonable steps to protect personal information held in the My Health Record system

In 2019–20, the OAIC concluded an assessment of the ADHA's handling of personal information. The assessment focused on APP 11, which requires the ADHA to take reasonable steps to protect personal information held in the My Health Record system, and on the relevant provisions in the My Health Records Act. The OAIC made 8 recommendations. The ADHA fully implemented 7 recommendations and agreed with the intent of 1 recommendation taking the view that the intended outcome was achieved through their assurance activities.

Assessment of 2 private hospitals — access controls for the My Health Record system

In 2019–20, the OAIC concluded an assessment of 2 private hospitals and their access controls for the My Health Record system. The assessment examined whether the hospitals had appropriate governance and information security arrangements to manage access security risks in accordance with Rule 42 of the My Health Records Rule and APPs 1.2 and 11. The OAIC made 22 recommendations to the 2 private hospitals, with all but 1 recommendation being fully adopted, the remaining recommendation being adopted in part.

Assessment of 14 pharmacies — access controls for the My Health Record system

In 2019–20, the OAIC concluded an assessment of 14 pharmacies and their access controls for the My Health Record system. The assessment involved a self-administered questionnaire and desktop review of documentation. It examined whether the pharmacies had appropriate governance and information security arrangements to manage access security risks in accordance with Rule 42 of the My Health Records Rule and APPs 1.2 and 11. Each of the pharmacies was individually advised about their assessment results. The results reflected a varied level of compliance across the targets.

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

In 2019–20, the OAIC continued an assessment of 8 pathology and diagnostic imaging services and their access controls for the My Health Record system. 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 APPs 1.2 and 11. The assessment was finalised for 7 of the 8 entities in 2019–20, with 1 assessment to be finalised in the 2020–21 reporting period. Each of the pathology and diagnostic imaging services was individually advised about their assessment results. Again, the results reflected a varied level of compliance across the targets.

A de-identified summary report combining the findings for the pharmacies assessment and the pathology and diagnostic imaging services assessment will be published in the 2020–21 reporting period. It will be accompanied by guidance for healthcare provider organisations with responsibilities and obligations under Rule 42.

Assessment of mobile health apps

In 2019–20, the OAIC commenced an assessment 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 APPs 1.2 and 5. This assessment will be finalised in the 2020–21 reporting period.

Data breach notifications

In 2019–20, the OAIC received 1 data breach notification from the ADHA. We closed 6 data breach notifications received from Services Australia (formerly known as the Department of Human Services) in 2018–19 during this reporting period.

Data breach notifications summary

Table 3: Data breach notifications

	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	–	–	1	–	–
Services Australia	–	–	–	6	12	6

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

Advice

My Health Record system enquiries

The OAIC's enquiries team received 6 telephone enquiries and 1 written enquiry about the My Health Record system during the reporting period.

Policy advice to stakeholders and members of the public

During the reporting period, the OAIC provided 20 policy advices to various stakeholders related to the My Health Record system. These included:

- comments to the Department of Health regarding its review of *Healthcare Identifier Regulations 2010*
- presentation to the ADHA's professional indemnity insurers workshop about 'Trends and experiences in health data privacy' in November 2019
- engagement with the Singaporean Ministry of Health regarding Australia's approach to digital health matters and the OAIC's role as regulator of the My Health Record system
- engagement with Queensland Health regarding a national framework for mobile health apps
- feedback to the Cyber Security Communication Coordination group regarding a draft data breach action plan for health sector businesses.

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:

- 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 with KPMG to discuss a compliance framework and with Information Integrity Solutions to discuss the ADHA's end-to-end privacy risk assessment of the system under the opt-out model
- comments on the ADHA's eLearning course on digital health security awareness
- advice regarding Privacy Impact Assessment (PIA) requirements under the *Privacy (Australian Government Agencies — Governance) APP Code 2017*
- advice regarding emergency declarations under the Privacy Act
- participation in a workshop in February 2020 to discuss the privacy aspects of the AHDA's operations and activities.

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 2019–20 we published the following resources:

- *Guide to health privacy* (September 2019)
- Privacy action plan for your health practice poster (October 2019)
- Data breach action plan for health service providers (February 2020).

For consumers

In July 2019, the OAIC launched a new website featuring a dedicated and easy-to-find 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 consumer-facing privacy resources through our social media channels.

Other external engagement

The OAIC is a member of the Cyber Security Communication Coordination Group, with the Australian Cyber Security Centre, the ADHA and Services Australia. In 2019–20, the group jointly developed and promoted a data breach action plan for health service providers, featuring a four-step plan to contain and manage a data breach involving health information, including My Health Records. The OAIC engaged with peak bodies such as the Australian Medical Association and Royal Australian College of General Practitioners to encourage distribution of the resource to their members.

The OAIC responded to 3 media enquiries about the My Health Record system during 2019–20.

In the final quarter of the reporting period, our participation in events was limited by postponements and cancellations as a result of the COVID-19 pandemic.

Liaison

Liaison with the ADHA

The OAIC liaised regularly with the ADHA about matters relating to the My Health Record system as well as ADHA's implementation of the ANAO's recommendations following the ANAO's performance audit of the My Health Record system.

Liaison with other key stakeholders

The OAIC met the Department of Health to discuss its Practice Incentives Program (PIP) and to understand any potential risks from a privacy and My Health Record system perspective.

The OAIC engaged with the Australian Institute of Health and Welfare (AIHW) on 2 occasions where secondary use of My Health Record data was discussed.

Other activities

Strengthening internal expertise

Throughout 2019–20, the OAIC continued to develop internal expertise regarding its functions and powers in connection with the My Health Record system. This involved ensuring new staff received induction training in digital health and the OAIC's regulatory oversight role. New staff also received extensive on-the-job training to ensure they acquired the necessary digital health subject matter knowledge.

An internal governance program was developed to identify key risks related to the My Health Record system and an internal officer-level network was convened to meet on a fortnightly basis to share expertise and discuss emerging risks and mitigation strategies.

Monitoring developments in digital health and the My Health Record system

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:

- Health Informatics Society of Australia Conference, Melbourne (12–14 August 2019)
- AIHW's National Health Information Strategy (NHIS) Sydney consultation forum (3 March 2020)
- University of Sydney, Sydney Ideas podcast – 'Flip the clinic: The digital approach to mental health support' (8 April 2020)
- Australian Institute of Digital Health virtual COVID-19 conference – 'Virtual care and telehealth in action during a global pandemic' (24 April 2020)
- Australian Institute of Digital Health virtual COVID-19 conference –'Emerging from the COVID-19 pandemic' (26 June 2020).

Part 4: The OAIC and the Healthcare Identifiers Service

The OAIC handles enquiries and complaints in relation to the HI Service. We monitor developments relating to digital health and the HI Service so we can offer informed 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 My Health Record System Operator 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.

OAIC compliance and enforcement activities

Complaints relating to the HI Service

The OAIC received 3 complaints about healthcare identifiers in 2019–20 and finalised 5 complaints. One complaint from 2019–20 remains ongoing.

Investigations relating to the HI Service

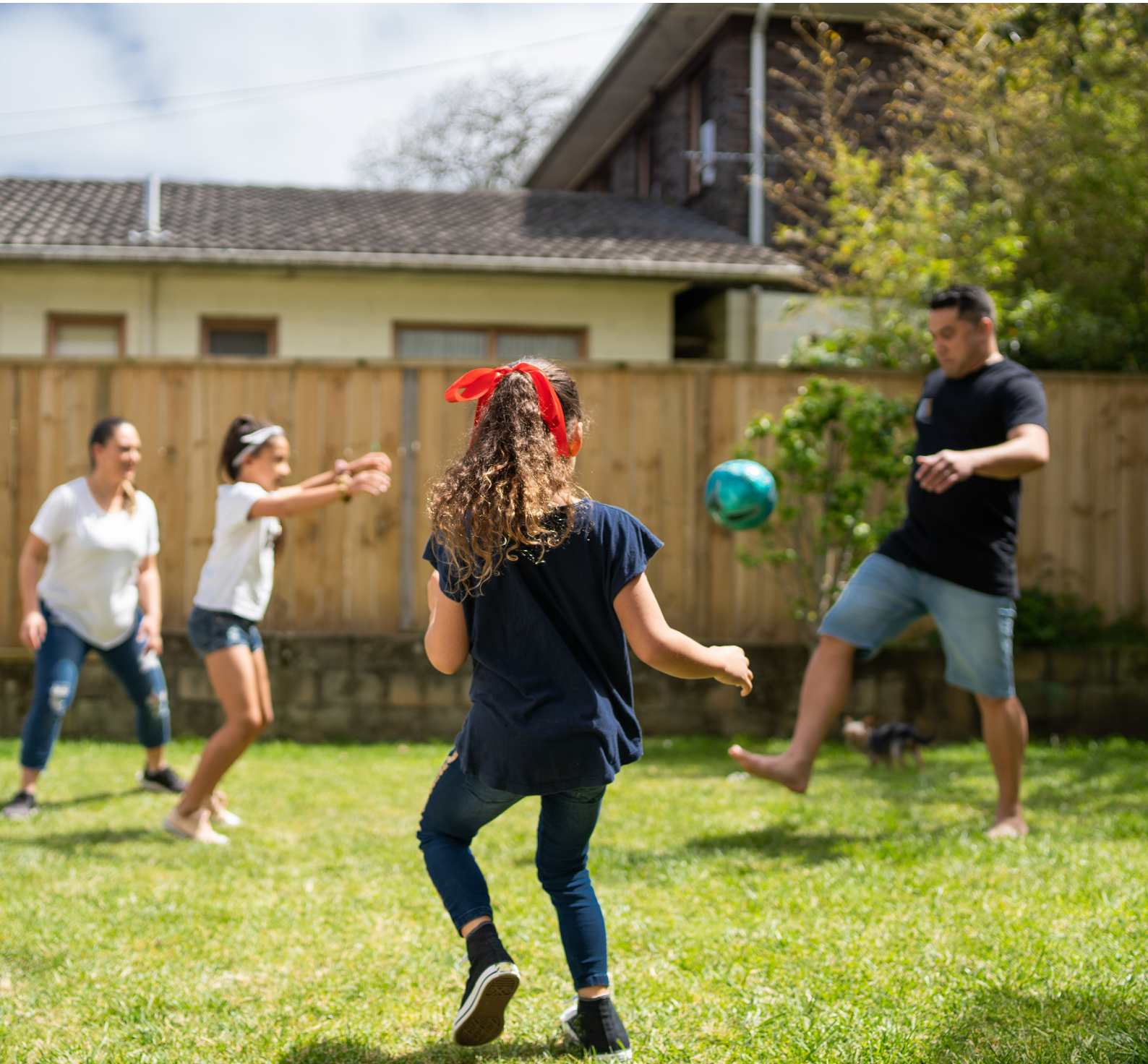
No complaint investigations or Commissioner-initiated investigations were commenced or finalised during the reporting period. At 30 June 2020, there were no HI Service investigations open.

Assessments relating to the HI Service

The OAIC did not initiate any assessments of the HI Service in 2019–20. The assessment program for this reporting period focused upon examining entities' adherence to privacy obligations related to the My Health Record system.

Table 4: Assessments relating to the HI Service in 2019–20

Assessment subject	Number of entities assessed	Year opened	Closed
Assessment of a private healthcare provider's handling of Individual Healthcare Identifiers — APP 11 and the HI Act	1	2017–18	Closed



HI Service advice, guidance, liaison and other activities

Advice

HI Service enquiries

The OAIC's enquiries team received 2 telephone enquiries about the HI Service during the reporting period.

Policy advice to stakeholders and members of the public

In relation to the HI Service, the OAIC provided comments to the Department of Health in response to its consultation paper regarding the review of the *Healthcare Identifiers Regulations 2010*.

The OAIC provided information about the HI Service to all new staff as part of our induction program.

Other activities

Monitoring developments in digital health and the HI Service

The OAIC monitors developments in digital health and the HI Service to ensure we are aware of the implications of any developments in relation to the HI Service and can 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.

Angelene Falk

Australian Information Commissioner
Australian Privacy Commissioner
24 September 2020

Australian Government

Office of the Australian Information Commissioner

Annual Report of the Australian Information Commissioner's activities in relation to digital health 2019–20

1300 363 992
enquiries@oaic.gov.au
@OAICgov

OAIC