The Auditor-General
Auditor-General Report No.13 2019–20
Performance Audit

Implementation of the My Health Record System

Australian Digital Health Agency

Department of Health

Australian National Audit Office

ISSN 1036–7632 (Print)
ISSN 2203–0352 (Online)
ISBN 978-1-76033-498-7 (Print)
ISBN 978-1-76033-499-4 (Online)

Senior Executive Director
Corporate Management Group
Australian National Audit Office
19 National Circuit
BARTON ACT 2600

Or via email:
communication@anao.gov.au.

Australian National
Audit Office

Canberra ACT

25 November 2019

Dear Mr President
Dear Mr Speaker

In accordance with the authority contained in the *Auditor-General Act 1997*, I have undertaken an independent performance audit in the Australian Digital Health Agency and the Department of Health. The report is titled *Implementation of the My Health Record System*. I present the report of this audit to the Parliament.

Following its presentation and receipt, the report will be placed on the Australian National Audit Office's website — http://www.anao.gov.au.

Yours sincerely

Grant Hehir
Auditor-General

The Honourable the President of the Senate
The Honourable the Speaker of the House of Representatives
Parliament House
Canberra ACT

AUDITING FOR AUSTRALIA

The Auditor-General is head of the Australian National Audit Office (ANAO). The ANAO assists the Auditor-General to carry out his duties under the *Auditor-General Act 1997* to undertake performance audits, financial statement audits and assurance reviews of Commonwealth public sector bodies and to provide independent reports and advice for the Parliament, the Australian Government and the community. The aim is to improve Commonwealth public sector administration and accountability.

For further information contact:
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Phone: (02) 6203 7300
Fax: (02) 6203 7777
Email: ag1@anao.gov.au

Auditor-General reports and information about the ANAO are available on our website:
http://www.anao.gov.au

Audit team

Scott Humphries
Christopher Swain
Barbara Das
Emily Drown
Emily Kilpatrick
David Brunoro

Contents

Audit snapshot

Auditor-General Report No.13 2019–20

Implementation of the My Health Record System

Why did we do this audit?

- My Health Record collates electronic summaries of individuals' health information so it can be accessed by the individual and different healthcare professionals involved in their care.
- The system is intended to generate benefits for individuals and the health system, but this requires balancing increased access to information with privacy and cyber security risks.

Key facts

- The system was 'opt-in' from 2012 and became 'opt-out' in 2019.
- Consumers can control access to their information, but their controls can be overridden in an emergency.
- Privacy and cyber risks are shared with many stakeholders including healthcare providers and IT vendors.

What did we conclude?

- Implementation of My Health Record has been largely effective.
- Implementation planning, governance and communication was appropriate.
- Risks relating to privacy and the IT core infrastructure were largely well managed, but management of shared cyber security risks was not appropriate and should be improved.
- Monitoring and evaluation was largely appropriate, but future planning for this could be improved.

What did we recommend?

- The Auditor-General made five recommendations to improve risk management and evaluation.
- The Australian Digital Health Agency and the Department of Health agreed with the recommendations.

$1.15 billion

Invested by government from 2012 to 2016 – with a further $374.2 million from 2017 to 2020.

90%

9 out of 10 Australians now have a My Health Record.

24%

16,400 healthcare provider organisations using the system.

Summary and recommendations

Background

1. My Health Record is an online electronic summary of a person's health information. The Australian Government invested $1.15 billion in the development of the system and other digital health infrastructure between 2012 and 2016. In the 2017–18 Budget, the government allocated a further $374.2 million to continue operating the system and expand its use by making it an opt-out model. Nine out of every ten Australians now has a My Health Record.

2. The Department of Health established the My Health Record system in 2012, and administers the *My Health Records Act 2012* on behalf of the Minister for Health. In July 2016, the Australian Digital Health Agency (ADHA) was prescribed as the System Operator for My Health Record.

Rationale for undertaking the audit

3. My Health Record potentially impacts all Australians as it collates electronic summaries of individuals' health information so it can be accessed by different healthcare professionals involved in a person's care (as well as by the individual themselves). The system is intended to generate personal benefits for individuals and economic benefits for the health system, but achieving this requires a balance between increasing access to information and managing privacy and cyber security risks. The system has also generated parliamentary and public interest in relation to privacy and cyber security risks.

Audit objective and criteria

4. The audit objective was to assess the effectiveness of the implementation of the My Health Record system under the opt-out model. The audit adopted the following criteria:

- implementation of the My Health Record system promotes achievement of its purposes;
- My Health Record system risks are appropriately assessed, managed and monitored; and
- monitoring and evaluation arrangements for the My Health Record system are effective.

5. The audit did not examine the decisions to create the My Health Record system or adopt the opt-out model, or consider the framework for secondary use of My Health Record data. No individual My Health Records were examined.

Conclusion

6. Implementation of the My Health Record system was largely effective.

7. Implementation planning for and delivery of My Health Record under the opt-out model was effective in promoting achievement of its purposes. Implementation planning and execution was appropriate, and was supported by appropriate governance arrangements. Communication activities were appropriate to inform healthcare recipients and providers.

8. Risk management for the My Health Record expansion program was partially appropriate. Risks relating to privacy and the IT system core infrastructure were largely well managed, and were informed by several privacy risk assessments and the implementation of key cyber security

measures. Management of shared cyber security risks was not appropriate and should be improved with respect to those risks that are shared with third party software vendors and healthcare provider organisations.

9. The monitoring and evaluation arrangements for My Health Record are largely appropriate. There are appropriate mechanisms to improve the quality of information entered into the system. Some benefits measurement activities are underway, but they are not yet organised in a research delivery and evaluation plan setting out milestones, timeframes and sequencing of activities over forward years.

Supporting findings

Implementation planning and delivery

10. The objectives of the My Health Record system were clearly specified in the legislation that enabled establishment of the My Health Record system. The objectives were translated to operational objectives in corporate planning documents.

11. Implementation governance arrangements were clear and appropriate. ADHA established clear governance structures for the My Health Record expansion program, including a dedicated program board and program delivery committee. Progress reports were provided to the majority of ADHA Board meetings.

12. Implementation planning was appropriate. The My Health Record expansion to an opt-out model was implemented in accordance with an approved business case and implementation plan. The plan was revised and updated as needed. Milestones identified in the implementation plan were achieved and reporting to the ADHA Board indicates the program was delivered within the approved program budget.

13. Communication strategies were appropriate. A communications strategy was developed in September 2017, informed by the participation trials evaluation and supplementary market research. The strategy included development, testing and production of materials such as brochures, posters, and videos aimed at different target groups. ADHA commissioned communication tracking which showed that ‘every Australian’ had on average 38 opportunities to see or hear about My Health Record within the opt-out period, and that awareness increased throughout the opt-out period. ADHA also delivered education activities for healthcare providers. Tracking results showed that all general practices and community pharmacies in Australia received access to some form of My Health Record education activities, and that this corresponded with increasing registration and use of the system.

Risk management

14. Governance of risk assessment, management and monitoring for the My Health Record expansion program was largely appropriate. ADHA had a risk management framework in place, supported by various assessments and registers at the whole-of-entity level and specifically for the My Health Record expansion program. Risk documentation could further mature (as noted in the 2019 gateway review), and the ADHA could also clarify the roles and responsibilities of other government entities in the management of shared risks.

15. ADHA's management of privacy risks was largely appropriate. Health and ADHA conducted several privacy impact assessments up until 2017 and implemented system and consumer access controls. System controls included access requirements for healthcare provider organisations and various consumer controls (including identity verification requirements, the ability to set advanced access controls and the ability to permanently delete records).

16. The ADHA has not yet undertaken an end-to-end privacy risk assessment of the ongoing operation of the My Health Record system under the opt-out model. The last privacy specific risk assessment was completed in 2017 and although ADHA funded the Office of the Australian Information Commissioner to conduct at least four privacy reviews between October 2017 and June 2019, none were completed in that period.

17. ADHA did not have sufficient assurance arrangements to satisfy itself that all instances of the emergency access did not constitute an interference with privacy. It should therefore review its approach and procedures for notifying the Information Commissioner of potential contraventions.

18. ADHA had largely appropriate systems to manage cyber security risks to the core infrastructure of the My Health Record system, except its management of shared cyber security risks and its oversight processes should be improved. ADHA managed risks to the core infrastructure through: establishing a Digital Health Cyber Security Centre; undertaking a series of dedicated cyber security assessments; and implementing the 'Essential Eight' cyber security mitigation strategies and decreasing the number of Information Security Manual (ISM) cyber security controls not implemented. ADHA's approach to managing shared cyber security risks was not appropriate. This should be improved by:

- developing an assurance framework for third party software connecting to the My Health Record system in accordance with the ISM; and
- developing a strategy to monitor compliance with legislated security requirements by registered healthcare provider organisations.

19. Cyber security risk oversight by the AHDA Board and its Privacy and Security Advisory Committee could also be strengthened. The ADHA Board received dedicated cyber security briefings on only four occasions between July 2016 and February 2019, and has not considered the updated 2019–2023 cyber security strategic plan (which was finalised by the ADHA executive on 14 November 2018). The role of the Privacy and Security Advisory Committee in cyber security was not clear.

Monitoring and evaluation

20. There are appropriate mechanisms to improve the quality of information entered into the system, such as: procedures to detect and correct administrative data errors; processes to promote consistency in how information is entered into the system; and data quality education and training activities. Work to monitor and improve data quality will need to continue as use of the system increases, especially if different types of users, who may not have accessed awareness and education activities, increase their participation over the coming years (such as medical specialists, allied health and aged care providers).

21. Arrangements to measure, evaluate and report on benefits realised from My Health Record are largely appropriate. A 2017 benefits realisation plan estimated benefits over a ten year

period, and identified potential data collection and research activities to measure the intermediate outputs and longer-term ('end') benefits.

22. ADHA is measuring intermediate outputs – which relate to participation and use of the system – and has commissioned some research activities to measure some longer-term benefits. These research activities are not yet organised within a plan setting out clear milestones, timeframes and sequencing of evaluation and reporting activities over the forward years.

Recommendations

Recommendation no. 1
Paragraph 3.27

ADHA conduct an end-to-end privacy risk assessment of the operation of the My Health Record system under the opt-out model, including shared risks and mitigation controls, and incorporate the results of this assessment into the risk management framework for the My Health Record system.

Australian Digital Health Agency response: *Agreed.*

Recommendation no. 2
Paragraph 3.45

ADHA, with the Department of Health and in consultation with the Information Commissioner, review the adequacy of its approach and procedures for monitoring use of the emergency access function and notifying the Information Commissioner of potential and actual contraventions.

Australian Digital Health Agency response: *Agreed.*

Department of Health response: *Agreed.*

Recommendation no. 3
Paragraph 3.76

ADHA develop an assurance framework for third party software connecting to the My Health Record system — including clinical software and mobile applications — in accordance with the Information Security Manual.

Australian Digital Health Agency response: *Agreed.*

Recommendation no. 4
Paragraph 3.82

ADHA develop, implement and regularly report on a strategy to monitor compliance with mandatory legislated security requirements by registered healthcare provider organisations and contracted service providers.

Australian Digital Health Agency response: *Agreed.*

Recommendation no. 5
Paragraph 4.29

ADHA develop and implement a program evaluation plan for My Health Record, including forward timeframes and sequencing of measurement and evaluation activities across the coming years, and report on the outcomes of benefits evaluation.

Australian Digital Health Agency response: *Agreed.*

Summary of entity responses

23. Summary responses from the selected entities are provided below, while the full responses are provided at Appendix 1.

Australian Digital Health Agency

> The Australian Digital Health Agency (Agency) welcomes the findings in the report and agrees with all recommendations made by the ANAO.
>
> The ANAO's conclusion that the implementation of the My Health Record was largely effective and that planning, governance and communication was appropriate will provide the community with an important perspective on the competence of the public sector to implement a system of this scale and nature. We support the sharing of learnings as key messages to other government entities. We hope that our experience implementing this major program will contribute to the capability of the public service to deliver major technological and change programs into the future.
>
> The Agency will work with Commonwealth entities, State and Territory Governments, healthcare providers and professionals, the technology industry and consumer groups to implement the recommendations.
>
> We acknowledge that the My Health Record operates within an environment of controls such as professional standards, national and State/Territory privacy laws, and risk systems that reduce exposure to adverse events. We will have regard to this complex environment when working with stakeholders to raise standards in health information management, with a view to lift the capability of the health sector to continue to meet increasing community expectations on privacy and the security of health information.
>
> We will continue to support the health and wellbeing of the Australian community through improved access to digital services.

Department of Health

> The Department of Health (the department) welcomes the findings in the report and, in particular notes the Auditor-General found the implementation of My Health Record has been largely effective. The audit also found the associated implementation planning, governance and communication were appropriate and risks relating to privacy and the IT core infrastructure were largely well managed.
>
> The department welcomes the recommendation identifying where improvements can be made and is committed to working with the Australian Digital Health Agency and the Office of the Australian Information Commissioner to support the implementation of the recommendations. The department is equally committed to protecting the privacy and security of people's health information and continues to engage with stakeholders to ensure the system remains safe and secure for users into the future.

Office of the Australian Information Commissioner

> The Office of the Australian Information Commissioner (OAIC) is the independent regulator of the privacy aspects of the My Health Record System. The OAIC provides advice, assistance and independently regulates the handling and management of personal information and Healthcare Identifiers in relation to and within the My Health Record system under a Memorandum of Understanding (MOU) with the Australian Digital Health Agency (ADHA). The OAIC's activities

under this MOU are set out in annual reports tabled in parliament and published on the OAIC's website.

The OAIC provided feedback to the ANAO on excerpts of a draft version of this report that contained references to the OAIC. The OAIC will consider the findings of this report as part of its ongoing regulatory role.

Key messages from this audit for all Australian Government entities

24. Below is a summary of key messages, including instances of good practice, which have been identified in this audit that may be relevant for the operations of other Australian Government entities.

Governance and risk management

My Health Record is an example of a program with many shared risks, not only between different Commonwealth agencies but also jurisdictions and the wider community, including the healthcare sector, clinical software vendors, and consumers. Good risk management is not just about managing risks to Commonwealth agencies; entities must also identify, assess and manage the risks that they share with others – which may include the groups of people to whom they are delivering services.

Performance and impact measurement

The intended benefits for the My Health Record system are estimated to take at least ten years to be realised. Where the intended benefits of a program are projected to be realised over a relatively long period, entities should not only describe what the intended benefits are and how they could be measured, but also make clear delivery plans showing how and when the benefits will be measured, evaluated and reported.

Audit findings

1. Background

Introduction

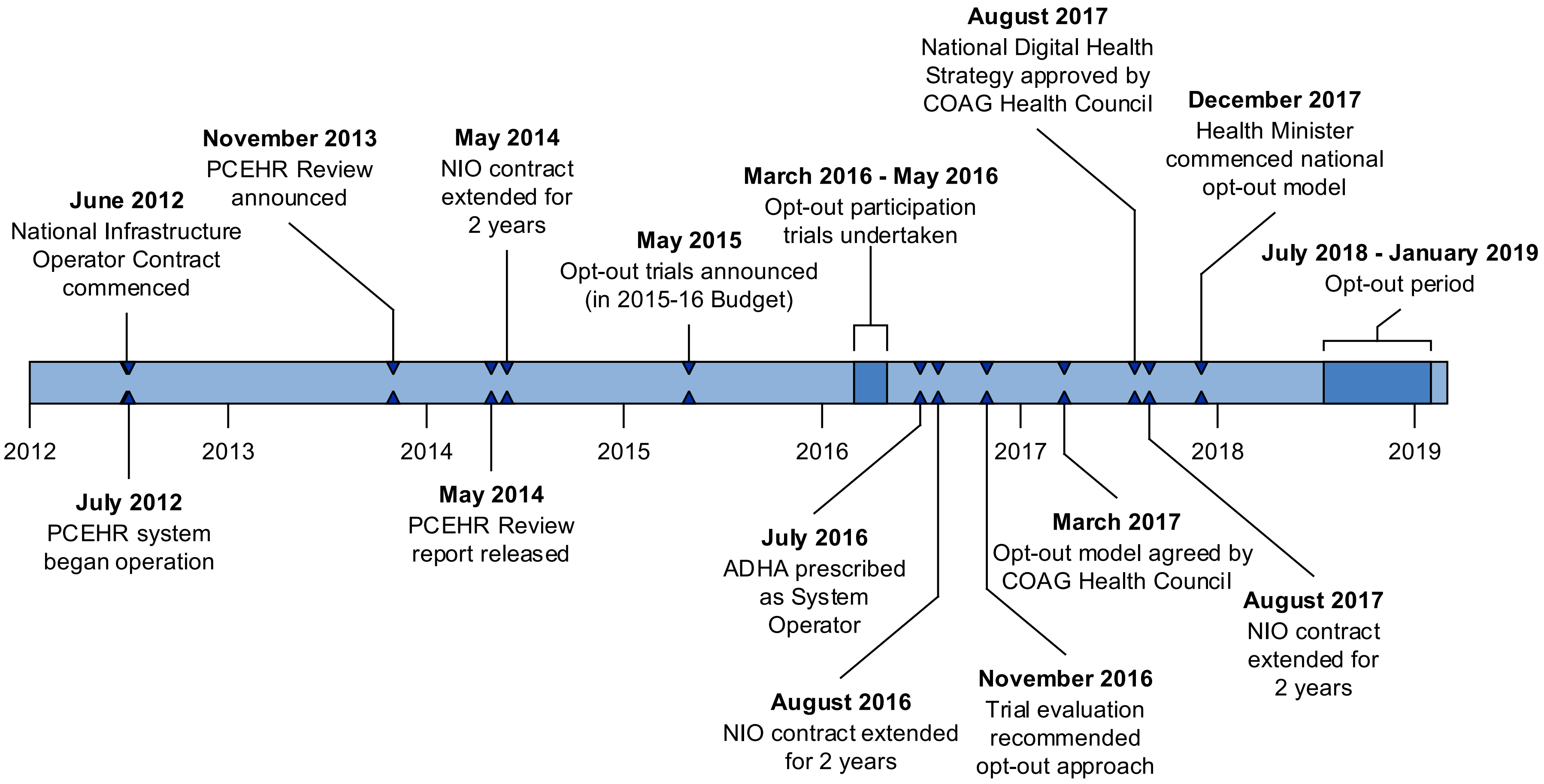
1.1 On 31 January 2019, the opt-out period for the My Health Record system concluded, marking a milestone in the establishment over two decades of a national system of access to electronic health records. On 22 February 2019, the System Operator for the My Health Record system — the Australian Digital Health Agency (ADHA) — announced that nine out of ten Australians would have a My Health Record.

My Health Record

1.2 Previously known as the Personally Controlled Electronic Health Record (PCEHR), My Health Record is an online electronic summary of a person's health information. It is a key element of a national digital health agenda to facilitate better sharing of health information across healthcare settings.[1] Following a 2013 review the PCEHR was renamed My Health Record, and, following participation trials in 2016, the government decided to transition the system from an 'opt-in' to an 'opt-out' model for healthcare recipients. Figure 1.1 presents the timeline of key developments for My Health Record from July 2012 to January 2019.

[1] Explanatory Statement, *Public Governance, Performance and Accountability (Establishing the Australian Digital Health Agency) Rule 2016* item 9..

Figure 1.1: Timeline of My Health Record 2012–2019

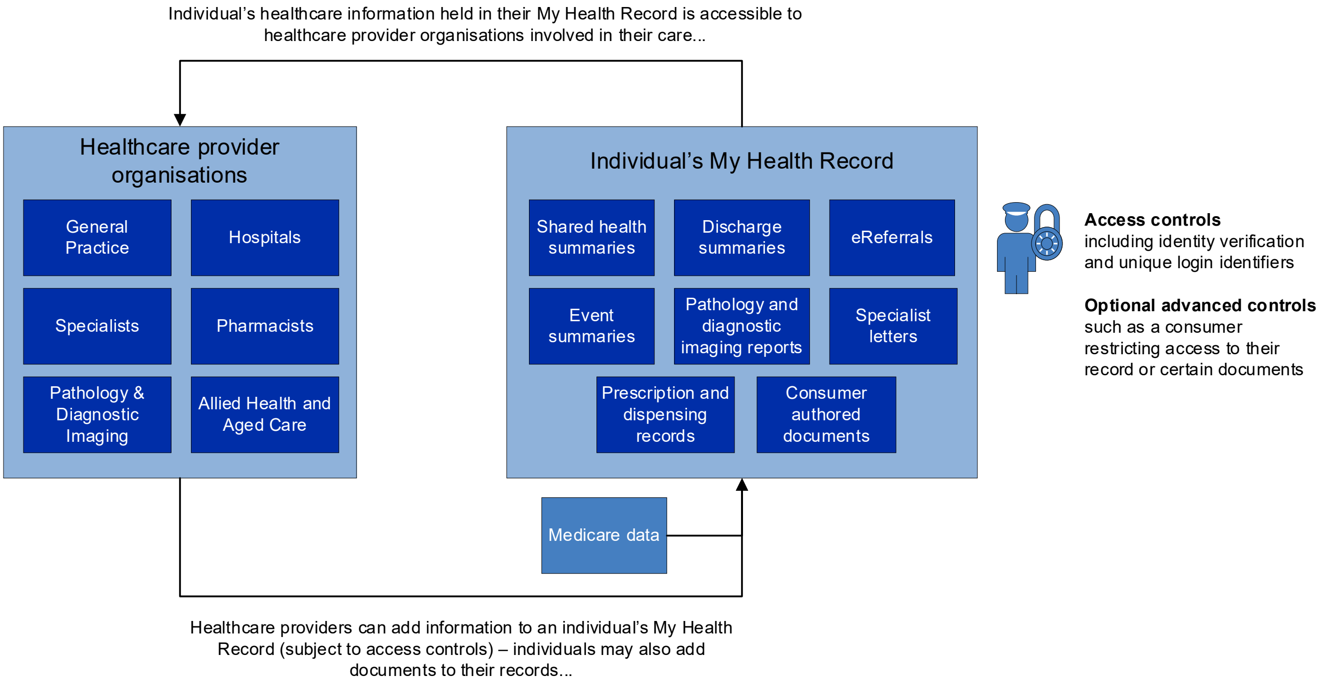

June 2012
National Infrastructure Operator Contract commenced
November 2013
PCEHR Review announced
May 2014
NIO contract extended for 2 years
May 2015
Opt-out trials announced (in 2015-16 Budget)
March 2016 - May 2016
Opt-out participation trials undertaken
August 2017
National Digital Health Strategy approved by COAG Health Council
December 2017
Health Minister commenced national opt-out model
July 2018 - January 2019
Opt-out period
2012
2013
2014
2015
2016
2017
2018
2019
July 2012
PCEHR system began operation
May 2014
PCEHR Review report released
July 2016
ADHA prescribed as System Operator
August 2016
NIO contract extended for 2 years
November 2016
Trial evaluation recommended opt-out approach
March 2017
Opt-out model agreed by COAG Health Council
August 2017
NIO contract extended for 2 years

Source: ANAO analysis of Australian Digital Health Agency and Department of Health documentation.

1.3 As illustrated in Figure 1.2, individual My Health Records may include:

- information from healthcare providers — health summaries, hospital discharge summaries, pathology and diagnostic imaging reports, medications, and referral letters; [2]
- information from repository operators — Medicare data, Pharmaceutical Benefits Scheme/Repatriation Pharmaceutical Benefits Scheme data, Australian Organ Donor Register decisions, and Australian Immunisation Register data;
- information added by healthcare recipients — such as contact numbers, emergency contact details, and advance care plans; and
- back-up copies of documents.[3]

Figure 1.2: How does My Health Record work?


Individual's healthcare information held in their My Health Record is accessible to healthcare provider organisations involved in their care...
Healthcare provider organisations
General Practice
Hospitals
Specialists
Pharmacists
Pathology & Diagnostic Imaging
Allied Health and Aged Care
Individual's My Health Record
Shared health summaries
Discharge summaries
eReferrals
Event summaries
Pathology and diagnostic imaging reports
Specialist letters
Prescription and dispensing records
Consumer authored documents
Medicare data
Access controls including identity verification and unique login identifiers
Optional advanced controls such as a consumer restricting access to their record or certain documents
Healthcare providers can add information to an individual's My Health Record (subject to access controls) – individuals may also add documents to their records...

Source: ANAO, based on Australian Digital Health Agency documentation.

1.4 My Health Records can be accessed by:

- healthcare recipients — who can view their My Health Record online through the myGov portal or through third party mobile applications;

[2] A 'shared health summary' is an overview description of a patient's status at a point in time. It may include medical history, conditions, medicines, allergies and immunisations. It is uploaded by the patient's nominated healthcare provider. A patient can have only one nominated healthcare provider at a time; other providers involved in the patient's care may instead use an 'event summary' to upload clinically relevant information.

Summarised from *Shared Health Summaries* [Internet], ADHA, https://www.myhealthrecord.gov.au/for-healthcare-professionals/howtos/shared-health-summaries [accessed 19 June 2019].

[3] Summarised from section 5 of *My Health Records Act 2012*; and Australian Digital Health Agency, *What's in a My Health Record?*, ADHA, [Internet],https://www.myhealthrecord.gov.au/for-you-your-family/whats-in-my-health-record [accessed 4 March 2019].

- healthcare providers — who can upload, view and share health information, subject to access controls set by the healthcare recipient;
- nominated representatives — who are chosen by healthcare recipients; and
- authorised representatives — who manage records for people who cannot manage their own.

Australian Government investment in My Health Record

1.5 The Australian Government invested $1.15 billion in developing the system and other digital health infrastructure between 2012 and 2016.[4] In the 2017–18 Budget, the government allocated a further $374.2 million to continue operating the system and expand its utilisation by making it an opt-out model. This was to be partially offset by savings for reduced duplication of pathology and diagnostic imaging claims on Medicare. At the time the 2017-18 Budget measure was developed potential economic benefits of $14.6 billion were identified in support of the Budget measure if the government was to invest $2.13 billion over ten years, including ongoing operating costs (as at June 2019, funding had only been allocated to 2020–21).[5]

Part of the National Digital Health Strategy

1.6 Implementation of My Health Record is one of seven strategic priorities in the National Digital Health Strategy, approved by the Council of Australian Governments (COAG) Health Council in August 2017 and being implemented by ADHA. The priorities are that:

- health information is available whenever and wherever it is needed;
- health information can be exchanged securely;
- high-quality data with a commonly understood meaning can be used with confidence;
- there is better availability and access to prescriptions and medicines information;
- digitally-enabled models of care improve accessibility, quality, safety and efficiency;
- the health workforce confidently uses digital health technologies to deliver care; and
- there is a thriving digital health industry delivering world class innovation.

Department of Health and Australian Digital Health Agency

1.7 The Minister for Health administers the *My Health Records Act 2012*. The Minister is supported by the Department of Health. The Department provides legislative support to ADHA, participates in system governance, and coordinates advice to government.

[4] The states and territories also provide funding for the Australian Digital Health Agency and the National Digital Health Strategy, as well as in kind contributions for My Health Record (for example, through provision of clinical content and delivery of digital health training for healthcare providers in the public sector).

[5] Funding allocated for 2020–21 was allocated subsequent to the 2017–18 Budget measure. Potential economic benefits and costs, which were not adjusted for the extended opt-out period, assumed the following My Health Record performance by 2020– 21: consumer participation rate of 98 per cent (participation rate was 90.1 per cent at July 2019); and GP registration rate of 90 per cent (86 per cent at July 2019).

1.8 ADHA was established as a corporate Commonwealth entity on 30 January 2016, and prescribed as the System Operator on 1 July 2016.[6] ADHA took over functions from the National E-Health Transition Authority (NEHTA) and system operation from the Department of Health.

1.9 The accountable authority for ADHA is the ADHA Board. The Board has four advisory committees (Clinical and Technical; Jurisdictional; Consumer; and Privacy and Security).[7] The Board has also established two additional advisory committees (Digital Health Safety and Quality Governance; and Audit and Risk).

1.10 As well as the Department of Health, ADHA works with other Australian Government agencies to deliver My Health Record, including:

- Services Australia — which provides the Healthcare Identifiers Service, Medicare data repositories, and information technology including the myGov access point for the My Health Record system;[8] and
- Office of the Australian Information Commissioner (OAIC) — which ADHA funds to provide advice and a regulatory service for the handling and management of personal information in the My Health Record system.[9]

1.11 A contracted National Infrastructure Operator (NIO) provides the technology platform for the My Health Record system and associated operation, maintenance, support and integration services. The contract has been held by the same service provider since 2012.[10] The initial two-year term included several extension options, all of which were used. At the time of the audit, ADHA was negotiating a further extension to 30 June 2022. Planning for the procurement process for future NIO arrangements (beyond June 2022) was underway during the period of the audit. That process will be subject to gateway reviews. A generic handover plan to transition to an alternative NIO was last updated in May 2019.

1.12 The roles played by these entities and other stakeholders are reflected in Figure 1.3.[11]

[6] The ADHA was prescribed to be the System Operator under the *My Health Records Regulation 2012*, paragraph 2.1.1. The *My Health Records Act 2012*, Part 2 sets out the identification and functions of the System Operator.

[7] These committees were established under the *Public Governance, Performance and Accountability (Establishing the Australian Digital Health Agency) Rule 2016*, Part 6.

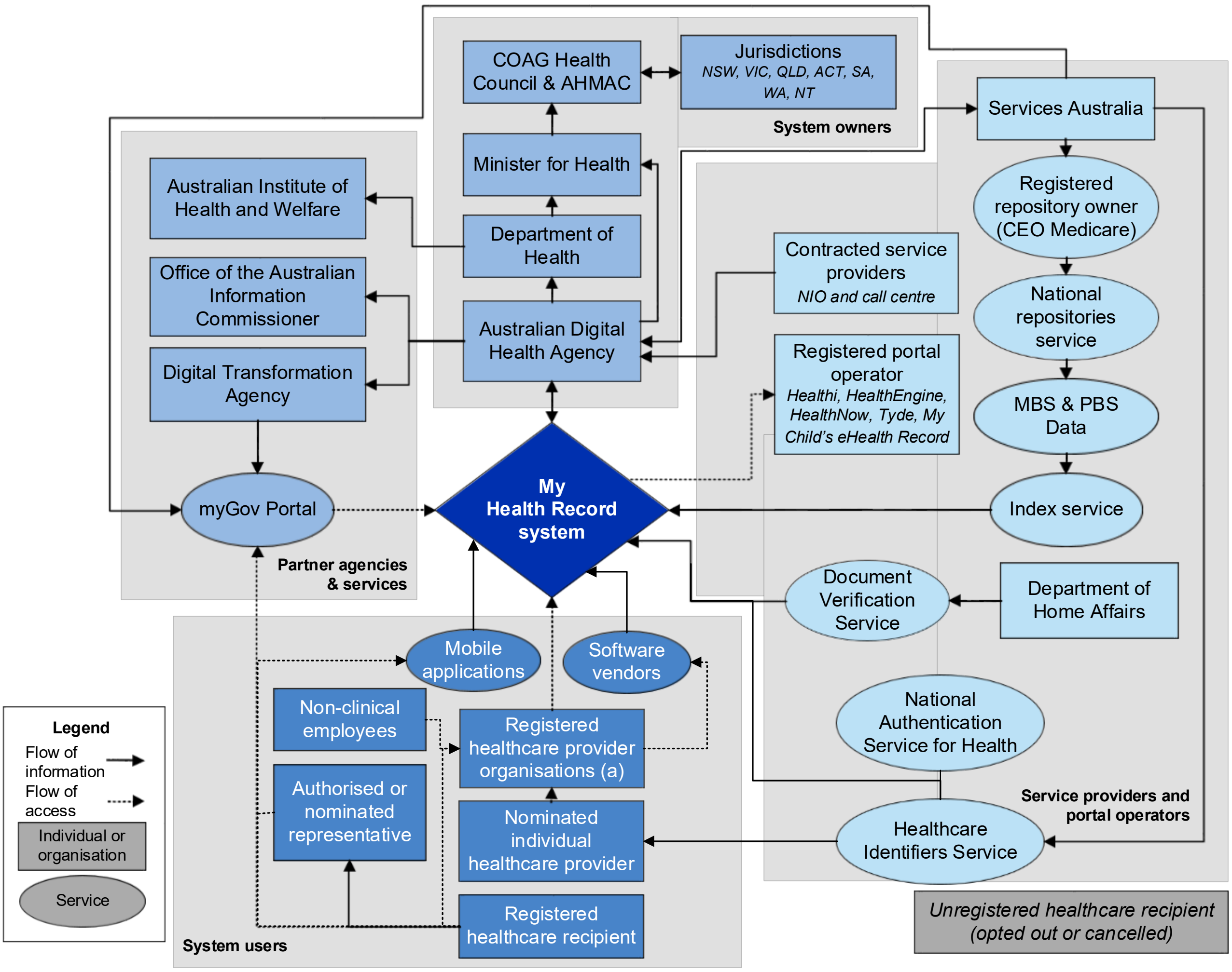
[8] Formerly the Department of Human Services until machinery of government changes on 29 May 2019.

[9] Under section 73 of the *My Health Records Act 2012*, and in addition to the Information Commissioner's functions under the *Privacy Act 1988*, the Information Commissioner has specific functions in relation to the My Health Record system to investigate potential interference with the privacy of a healthcare recipient. The Information Commissioner is also the independent regulator of the privacy aspects of the *Healthcare Identifiers Regulations 2010*. The healthcare identifiers legislation implements a national system for assigning identifiers to healthcare recipients, healthcare providers, and healthcare provider organisations.

[10] Health transferred management of the contract to ADHA in July 2016.

[11] Health services operated by state/territory jurisdictions participate in the My Health Record system as healthcare provider organisations.

Figure 1.3: Roles of Australian Government entities and other stakeholders


COAG Health Council & AHMAC
Jurisdictions
NSW, VIC, QLD, ACT, SA, WA, NT
System owners
Services Australia
Minister for Health
Registered repository owner (CEO Medicare)
Australian Institute of Health and Welfare
Department of Health
Contracted service providers
NIO and call centre
Office of the Australian Information Commissioner
National repositories service
Australian Digital Health Agency
Registered portal operator
Healthi, HealthEngine, HealthNow, Tyde, My Child's eHealth Record
Digital Transformation Agency
MBS & PBS Data
My Health Record system
myGov Portal
Index service
Partner agencies & services
Document Verification Service
Department of Home Affairs
Mobile applications
Software vendors
Legend
Flow of information
Flow of access
Individual or organisation
Service
Non-clinical employees
Registered healthcare provider organisations (a)
National Authentication Service for Health
Authorised or nominated representative
Service providers and portal operators
Nominated individual healthcare provider
Healthcare Identifiers Service
Registered healthcare recipient
Unregistered healthcare recipient (opted out or cancelled)
System users

Note a: Health services operated by jurisdictions participate in the My Health Record system as registered healthcare provider organisations.

Source: ANAO.

Basis for the 'opt-out' model

1.13 The PCEHR was an 'opt-in' system for healthcare recipients and providers. Amendments to the *My Health Records Act 2012* in November 2015 enabled the system to operate on an 'opt-out' basis for healthcare recipients, and for the Minister for Health, in consultation with state and territory health ministers, to apply the opt-out model through trials and nationally if 'the Minister decides that the opt-out model results in participation in the My Health Record system at a level that provides value for those using the My Health Record system'.[12]

1.14 From March to May 2016, My Health Record opt-out trials were held in the Northern Queensland and Nepean Blue Mountains Primary Health Networks. The trial evaluation

[12] *My Health Records Act 2012*, Schedule 1, clause 2, inserted in 2015.

recommended that 'government proceed to a national opt-out approach'.[13] The COAG Health Council agreed to a national opt-out model on 24 March 2017. The Minister for Health commenced the national opt-out model from 2 December 2017.[14]

1.15 The opt-out model initially included a three-month 'opt-out period' during which healthcare recipients could choose not to be registered, after which the System Operator would register every eligible person.[15] This period was legislated to run from 16 July 2018 to 15 October 2018.

1.16 On 31 July 2018, the Minister for Health announced the government's intention to amend the legislation, on 10 August 2018 he announced that the opt-out period would be extended to 15 November 2018, and on 22 August 2018 the Minister introduced the My Health Records Amendment (Strengthening Privacy) Bill 2018 into the Parliament.

1.17 On 15 August 2018, the Senate referred the My Health Record system to the Senate Community Affairs References Committee. The committee tabled its inquiry report on 18 October 2018.[16] The report made 14 recommendations. By October 2019, a government response had not been tabled.

1.18 On 23 August 2018, the Senate referred the My Health Records Amendment (Strengthening Privacy) Bill 2018 to the Senate Community Affairs Legislation Committee. The committee tabled its inquiry report on 12 October 2018. The report recommended the Bill be passed, with minority reports raising issues around the scope of authorised disclosure and backup record destruction.

1.19 Following passage of the amendments by the Senate, the Minister for Health announced that the opt-out period would be extended to 31 January 2019. The amendments also implemented several changes that will come into effect in December 2019:

- enabling the My Health Records Rules to prescribe a framework to guide the collection, use and disclosure of de-identified data and, with the consent of healthcare recipients, health information, for research or public health purposes;
- appointing the Australian Institute of Health and Welfare as the My Health Record data custodian for research and public health purposes and creating a Data Governance Board to review applications for data use; and
- requiring the System Operator to comply with a direction from, and follow the guidance of, the Data Governance Board.[17]

1.20 The changes also required the System Operator to permanently delete health information stored in My Health Record when a healthcare recipient requests cancellation of their record.

[13] Siggins Miller, *Evaluation of the Participation Trials for the My Health Record*, Final Report, November 2016.

[14] The National Opt-out Rules in the *My Health Records (National Application) Rules 2017* state at section 5 that opt-out applies to all healthcare recipients in Australia. This provision commenced from 2 December 2017.

[15] *My Health Records (National Application) Rules 2017*, section 6.

[16] Community Affairs References Committee, *My Health Record system*, Commonwealth of Australia, 2018.

[17] The *Framework to Guide Secondary Use of My Health Record system data* outlines the membership and role of the Data Governance Board in chapter 1 (pages 14–15). Available from: https://www.health.gov.au/internet/main/publishing.nsf/Content/F98C37D22E65A79BCA2582820006F1CF/$File/MHR_2nd_Use_Framework_2018_ACC_AW3.pdf [accessed 12 June 2019].

1.21 On 22 February 2019, ADHA reported a national opt-out rate of 9.9 per cent. Statistics on use of the system at the end of opt-out and the end of July 2019 are presented in Table 1.1 .

Table 1.1: My Health Record statistics

End of opt out period (31 January 2019)	Progress at 28 July 2019
Participation Australians with a My Health Record: 90.1 per cent Healthcare provider organisations: 22.8 per cent[a]	**Participation** Australians with a My Health Record: 90.1 per cent Healthcare provider organisations: 24 per cent[a]
Core clinical content in the system Clinical documents uploaded: 11.5 million Medication records uploaded: 32 million Consumer documents uploaded: 224,224	**Core clinical content in the system** Clinical documents uploaded: 28 million Medication records uploaded: 64 million Consumer documents uploaded: 240,000

Note a: This figure includes all healthcare provider organisations including those with lower participation rates such as specialists, allied health and aged care. By contrast, at 28 July 2019, the participation rate for general practice was 86 per cent; public hospitals 75 per cent; pharmacies 85 per cent; and private hospitals 66 per cent.

Source: ANAO analysis of ADHA data

Rationale for undertaking the audit

1.22 The My Health Record system potentially impacts all Australians as it collates electronic summaries of individuals' health information so it can be accessed by different healthcare professionals involved in a person's care (as well as by the individual themselves). The system is intended to generate personal benefits for individuals and economic benefits for the health system, but achieving those intended benefits requires a balance between increasing access to information, and managing the inherent privacy and cyber security risks of making that information more readily available. For these reasons, My Health Record has generated parliamentary and public interest, particularly in relation to the management of privacy and cyber security risks.

Audit approach

Audit objective, criteria and scope

1.23 The audit objective was to assess the effectiveness of the implementation of the My Health Record system under the opt-out model. The following criteria were adopted:

- implementation of the My Health Record system promotes achievement of its purposes;
- My Health Record system risks are appropriately assessed, managed and monitored; and
- monitoring and evaluation arrangements for the My Health Record system are effective.

1.24 The audit did not examine the decisions to create the My Health Record system or adopt the opt-out model, or consider the framework for secondary use of My Health Record data.

Audit methodology

1.25 The audit team:

- examined ADHA and Department of Health information;
- reviewed the Senate Inquiries' final reports and individual submissions;

- interviewed ADHA and Department of Health staff; and
- interviewed Services Australia, Digital Transformation Agency, and Office of the Australian Information Commissioner staff.

1.26 The audit was open to citizen contributions, and received 20 contributions.

1.27 The audit team did not examine any individual My Health Records.

1.28 The audit was conducted in accordance with ANAO auditing standards at a cost to the ANAO of $612,670.

1.29 The team members for this audit were Scott Humphries, Christopher Swain, Barbara Das, Emily Drown, Emily Kilpatrick, and David Brunoro.

2. Implementation planning and delivery

Areas examined

This chapter examines whether the My Health Record system was implemented effectively to promote achievement of its purposes.

Conclusion

Implementation planning for and delivery of My Health Record under the opt-out model was effective in promoting achievement of its purposes. Implementation planning and execution was appropriate, and was supported by appropriate governance arrangements. Communication activities were appropriate to inform healthcare recipients and providers about My Health Record.

Areas for improvements

The ANAO did not make any recommendations in this chapter.

2.1 Section 15 of the *Public Governance, Performance and Accountability Act 2013* requires that accountable authorities must govern in a way that promotes the achievement of (an entity's) purpose. The audit examined how ADHA governed the program of work that implemented My Health Record as an 'opt-out' model (this work was referred to as the 'expansion program' by ADHA). The audit considered the effectiveness of the following four elements:

- whether the intended objectives of My Health Record were clearly specified in legislation and relevant planning documents;
- clarity of the My Health Record governance arrangements;
- appropriateness of the My Health Record implementation planning; and
- appropriateness of the communication strategies that informed people about My Health Record and the opt-out process.

Were objectives clearly specified?

The objectives of the My Health Record system were clearly specified in the legislation that enabled establishment of the My Health Record system. The longer-term legislative objectives were translated to operational objectives in corporate planning documents.

2.2 The *My Health Records Act 2012* enabled establishment of the My Health Record system. The object of the Act is to enable the establishment and operation of a voluntary national public system for the provision of access to health information relating to recipients of healthcare, to:

- help overcome the fragmentation of health information;
- improve the availability and quality of health information;
- reduce the occurrence of adverse medical events and the duplication of treatment; and
- improve the coordination and quality of healthcare provided to healthcare recipients by different healthcare providers.[18]

[18] Section 3 of the *My Health Records Act 2012* outlining the object of the Act was amended in 2015 and in 2018.

2.3 The rationale for the My Health Record system was based on the intended benefits of a single point of access to health information at the point of care. The Minister for Health stated in August 2018 that:

> Health information is spread across a vast number of different locations and systems. In many healthcare situations, quick access to key health information about an individual is not always possible. Limited access to health information at the point of care can result in a greater risk to patient safety, less than optimal health outcomes, avoidable adverse events, increased costs of care and time wasted in collecting or finding information, unnecessary or duplicated investigations, additional pressure on the health workforce, and reduced participation by individuals in their own healthcare management.[19]

2.4 The longer-term statutory objectives of the My Health Record system were translated into operational objectives in relevant corporate documents:

- the 2017–18 Portfolio Budget Statements for ADHA included performance criteria for 'delivering national opt-out for My Health Record', including communication and education activities, as well as improving participation, usage, content and engagement with the service through continued improvements and functionality;[20]
- the 2017–18 corporate plan for ADHA reflected these criteria in 'key milestones' that, by 2019, 'every Australian will have a My Health Record, unless they choose not to'. The plan also included targets to 'deliver a national opt-out model for the My Health Record system and enhance the system to improve participation, usage, content and engagement with the service', as well as increasing pathology and diagnostic imaging content.[21]

2.5 The corporate objectives were expanded upon in the implementation plans for delivering the opt-out model (discussed further from paragraph 2.10).

Were implementation governance arrangements clear and appropriate?

Implementation governance arrangements were clear and appropriate. ADHA established clear governance structures for the My Health Record expansion program, including a dedicated program board and program delivery committee. Progress reports were provided to the majority of ADHA Board meetings.

2.6 Effective governance arrangements start with having a clear purpose for the activity, which in this case was to implement the My Health Record system as an opt-out model.[22] ADHA established the 'My Health Record expansion program' to move My Health Record to an opt-out

[19] My Health Records Amendment (Strengthening Privacy) Bill 2018, Explanatory Memorandum, p. 1.

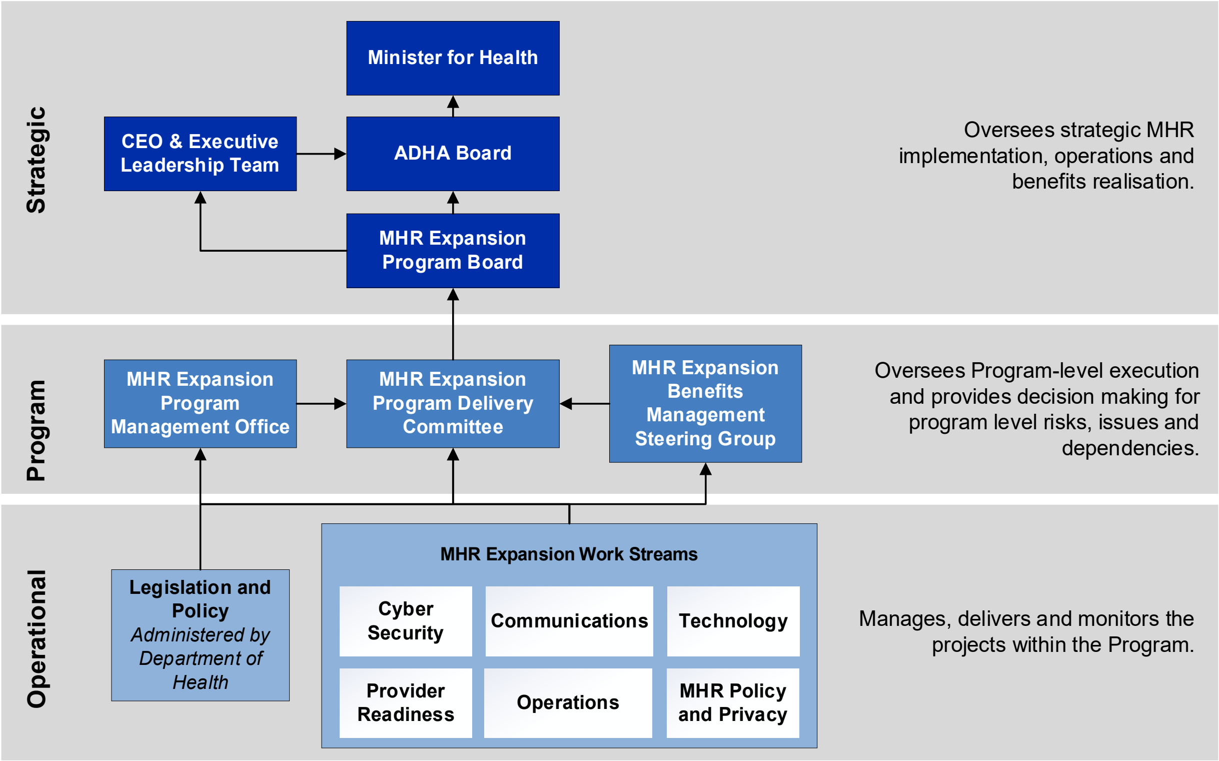
[20] Australian Government, *Portfolio Budget Statements 2017-18, Budget Related Paper No. 1.10, Health Portfolio*, pp.194–197.

[21] Australian Digital Health Agency, *Corporate Plan 2017–18*, p. 6, pp. 10–11, and pp.17–19.

[22] The Department of Finance has identified core principles for the design of governance structures for government activities, including clarity of purpose and optimisation of efficiency and performance. Department of Finance, *Core governance arrangements* [Internet] available from https://www.finance.gov.au/resource-management/governance/policy/principles/ [accessed June 2019].

model, under the direction of a program board that reported to the ADHA Board. This structure is reflected in Figure 2.1.

Figure 2.1: Implementation governance for the My Health Record expansion program


Strategic
Minister for Health
CEO & Executive Leadership Team
ADHA Board
MHR Expansion Program Board
Oversees strategic MHR implementation, operations and benefits realisation.
Program
MHR Expansion Program Management Office
MHR Expansion Program Delivery Committee
MHR Expansion Benefits Management Steering Group
Oversees Program-level execution and provides decision making for program level risks, issues and dependencies.
Operational
Legislation and Policy
Administered by Department of Health
MHR Expansion Work Streams
Cyber Security
Communications
Technology
Provider Readiness
Operations
MHR Policy and Privacy
Manages, delivers and monitors the projects within the Program.

Source: ANAO, adapted from Australian Digital Health Agency documentation.

2.7 There were clear program governance plans in place that set out the purpose of the My Health Record expansion program, with regular progress reporting to the ADHA Board. This reporting was at least quarterly, but in practice was more frequent with updates provided at 13 of 16 board meetings held between June 2017 and April 2019. Program governance committees had terms of reference and meetings were documented. Senior executive staff had clearly defined responsibilities and key procedures were documented.

2.8 The Department of Health undertook a review of ADHA governance and operations in December 2018.[23] The report was provided to the ADHA Board in April 2019, and made 14 recommendations relating to organisational structure (including rationalisation of ADHA Board advisory committees); formalising its relationship with Health (including through a service level agreement); implementing a skills-matrix for future ADHA Board appointments; and articulating a clear vision, purpose and KPIs at the entity-level. The ADHA stated to the ANAO that these recommendations are being considered by the ADHA Board.

[23] This review was commissioned by Health to inform the business case for future ADHA funding beyond 2020. Although called a 'functional and efficiency review', it was not a functional and efficiency review commissioned by the Department of Finance under the Efficiency through Contestability Program.

Was implementation planning appropriate?

Implementation planning was appropriate. The My Health Record expansion to an opt-out model was implemented in accordance with an approved business case and implementation plan. The plan was revised and updated as needed. Milestones identified in the implementation plan were achieved and reporting to the ADHA Board indicates the program was delivered within the approved program budget.

2.9 The Department of the Prime Minister and Cabinet (PM&C) requires an implementation plan for new policy and program proposals that have significant risks or challenges. PM&C recommends that implementation plans include key milestones, details of senior responsible officers, and details of key risks and mitigation strategies.[24]

2.10 In April 2017, the government approved a business case for the transition of My Health Record to an opt-out model (the My Health Record expansion program). The business case included an implementation plan that outlined administrative and governance structures for delivery of the My Health Record expansion program. The plan was adjusted in September 2018 to reflect timing and scope changes arising from ministerial decisions.

2.11 The plan outlined: objectives and outcomes for the opt-out process; timeframes, governance; project work required to deliver the expansion program; and project costings. The implementation plan was supported by several project work plans. A senior executive within ADHA was identified as the Senior Responsible Officer.

2.12 The expansion program was implemented in accordance with the implementation plan, and adjusted for changed timeframes associated with legislative changes including the opt-out period extension. Milestones were achieved on time – adjusted for the extended opt-out period – and reporting to the ADHA Board indicates the expansion program was delivered within the approved budget.[25]

2.13 The expansion program was subject to gateway reviews.[26] An initial review was conducted in October 2016, a mid-stage review in June 2017, and a final review in May 2019. The final review found that the expansion program had been implemented and that the My Health Record system design addressed key issues of data ownership, privacy and cyber security, noting that time and continued effort would be required to realise the benefits of the system. The review made five recommendations, of which two were for immediate action: to review and finalise risk management procedures, and to commence preparations for the approach to market for the future National Infrastructure Operator arrangements. In August 2019, ADHA stated to the ANAO that ADHA was

[24] Department of the Prime Minister and Cabinet, *Policy implementation,* [Internet], PM&C, available from https://www.pmc.gov.au/government/policy-implementation [accessed 3 September 2019].

[25] At 30 June 2019, the final actual spend for the expansion program was $231.9 million, with a small underspend against the total budget of $232.9 million. The total budget included additional funds allocated subsequent to the 2017 budget measure for the opt-out extension and additional communication activities.

[26] Gateway reviews are an independent assurance process that assist Commonwealth entities to deliver high risk projects and programs. They involve a series of short, intensive reviews at critical implementation points to provide independent assurance to the entity, and early identification of problems. Department of Finance, *Gateway reviews* [Internet] available from https://www.finance.gov.au/assurance-reviews/review-process/ [accessed August 2019].

actioning all of the recommendations, with the risk management procedures expected to be finalised by November 2019 and preparations for the approach to market underway (see paragraph 1.11).

Were communication strategies appropriate?

Communication strategies were appropriate. A communications strategy was developed in September 2017, informed by the participation trials evaluation and supplementary market research. The strategy included development, testing and production of materials such as brochures, posters, and videos aimed at different target groups. ADHA commissioned communication tracking which showed that 'every Australian' had on average 38 opportunities to see or hear about My Health Record within the opt-out period, and that awareness increased throughout the opt-out period. ADHA also delivered education activities for healthcare providers. Tracking results showed that all general practices and community pharmacies in Australia received access to some form of My Health Record education activities, and that this corresponded with increasing registration and use of the system.

2.14 The *My Health Records Act 2012* includes a role for the System Operator 'to educate healthcare recipients, participants in the My Health Record system and members of the public about the My Health Record system'.[27]

2.15 The *Guidelines on Information and Advertising Campaigns* outline principles for certain government communication campaigns.[28] ADHA is not subject to the guidelines, but stated to ANAO that it applied them in its communications planning.

2.16 A communications strategy was developed in September 2017. It was informed by the trial evaluation recommendations and supplementary market research. The initial budget for communication and engagement was $27.75 million. With the second extension of opt-out, a further $5 million was provided to add a national television advertising campaign.

2.17 The strategy identified a range of stakeholders including all persons with a Medicare number or Department of Veterans' Affairs card, state and territory health agencies, peak health organisations and clinician professional bodies, and healthcare providers. The strategy was supported by plans targeted to healthcare providers, general healthcare recipients, those in regional and remote areas, and those with special needs.[29]

2.18 ADHA commissioned the development, testing and production of materials such as brochures, posters, and videos aimed at different target groups. The Office of the Australian Information Commissioner and Department of Health provided feedback on those materials.

[27] Subsection 15(m) of the *My Health Records Act 2012.*

[28] Department of Finance, *Guidelines on Information and Advertising Campaigns by non-corporate Commonwealth entities* [Internet] available from https://www.finance.gov.au/sites/default/files/campaign-advertising-guidelines.pdf [accessed June 2019].

[29] Special needs included people from culturally and linguistically diverse backgrounds, people from Aboriginal and Torres Strait Islander backgrounds, people with disability, those experiencing homelessness or domestic violence, children in out of home care, adult prisoners, juvenile detainees, and various other groups.

Box 1: Examples of targeted communication activities for special need groups

- Consumer materials translated into 17 different languages
- Plain text factsheets for people with low literacy
- Auslan translation video for people who are hearing impaired
- Brochures and opt out forms provided in Australia Post offices in remote areas
- Engagement with housing and shelter groups for people experiencing homelessness

Source: ADHA.

2.19 Delivery of the strategy aligned with a recommendation from the trials evaluation to be 'nationally driven and locally delivered', utilising partnerships with Primary Health Networks (PHNs), states and territory government departments, peak health and community bodies, and professional bodies. The largest partnership was with PHNs, which were contracted to develop and deliver local communication activities using materials developed by ADHA. PHNs' plans were approved by ADHA and included various activities targeted to healthcare recipients and providers including general practice, pharmacists, public and private hospitals, specialists and allied health. Contracts included a schedule for delivery dates, KPIs and reporting. ADHA also delivered communications through its website and Services Australia channels (service centres, Your Health website, Medicare Online Account landing page, and social media).

2.20 The initial campaign did not include national television, print or outdoor advertising although there were some paid radio, social media and digital advertising placements, and regional television and print advertising linked to local PHN plans. The campaign instead aimed to provide information within community settings via healthcare providers, peak bodies and PHNs. Brochures were also included in Medicare letters mailed out during the opt-out period.

2.21 ADHA commissioned communication tracking which showed that 'every Australian' had on average 38 opportunities to see or hear about My Health Record within the opt-out period.[30] As shown in Table 2.1, awareness increased throughout the opt-out period.

Table 2.1: Healthcare recipient awareness of My Health Record and Opt-out

	June 2018	February 2019
Awareness of MHR	63.6%	92.1%
Awareness of Opt-out	16.5%	69.2%

Source: ANAO analysis of ADHA documentation.

2.22 Communication to the wider public about My Heath Record and opt-out was initially limited to a three month period between July 2018 and October 2018. This was later extended for a further three months to January 2019 following the extension by government of the opt-out period. At this point, television advertising was conducted in major cities and regional areas. ADHA had not initially included national television advertising in the strategy, and the potential risks of not undertaking 'above the line' communications were acknowledged in ADHA Board papers.

[30] Awareness tracking indicated no substantial difference related to geography or demography.

2.23 The trials evaluation had found that the most common source of awareness about My Health Record for healthcare recipients in opt-out trial sites was 'national media'[31], myGov, and 'Other' (including social media and word of mouth). Awareness tracking commissioned by ADHA during opt-out showed that, while at the beginning of the opt-out period, the most common source of information was healthcare settings (32 per cent), by the end of the period most people had heard about My Health Record via the media (75 per cent).

Education activities

2.24 ADHA also delivered education activities for healthcare providers to increase their awareness and understanding of My Health Record and its potential benefits, and their proficiency in using it. In the lead-up to and during opt-out these efforts focussed on general practitioners, pharmacists, hospitals, and diagnostic imaging and pathology services.

2.25 As with the communications, education activities were delivered through partnerships with jurisdictions, PHNs, professional bodies and medical colleges. Activities ranged from webinars and face-to-face training, to individual support for medical practices and development of learning modules with Continuing Professional Development points for general practitioners and pharmacists. Activities were delivered between October 2017 and June 2019.

2.26 ADHA tracked the progress of the funded education activities. The tracking results showed that all general practices and community pharmacies in Australia received access to some form of My Health Record education activities, and that this corresponded with increasing registration and use of the system (registrations exceeded targets of 80 per cent of general practices and 60 per cent of community pharmacies – at July 2019, 86 per cent of general practices were registered and 85 per cent of community pharmacies).[32]

2.27 Tracking also measured the number of shared health summary uploads to the system; the number of dispense record uploads; the number of event summary uploads; and the number of providers viewing record content, broken down by PHN region. This data showed an increase in record uploads and shares after delivery of the education activities.

[31] This term was not defined in the report.

[32] Education activities with specialists and allied health providers were also tracked.

3. Risk management

Areas examined

This chapter examines the appropriateness of risk management for the My Health Record system.

Conclusion

Risk management for the My Health Record expansion program was partially appropriate.

Risks relating to privacy and the IT system core infrastructure were largely well managed, and were informed by several privacy risk assessments and the implementation of key cyber security measures. Management of shared cyber security risks was not appropriate and should be improved with respect to risks that are shared with third party software vendors and healthcare provider organisations.

Areas for improvement

The ANAO made four recommendations aimed at improving privacy and cyber security risk management.

3.1 The appropriateness of risk management for My Health Record is a key consideration for this audit, particularly given the parliamentary and public interest in the privacy and cyber security risks that are inherent to the system. These risks are increased because they are shared with a number of other entities and individuals. The ANAO examined the governance and oversight of My Health Record risks, and more specifically the management of privacy and cyber security risks. Findings in this chapter are based on analysis of documentation and information obtained from the entity. The ANAO did not undertake independent testing of risk controls.

Is governance of risk assessment, management and monitoring appropriate?

Governance of risk assessment, management and monitoring for the My Health Record expansion program was largely appropriate. ADHA had a risk management framework in place, supported by various assessments and registers at the whole-of-entity level and specifically for the My Health Record expansion program. Risk documentation could further mature (as noted in the 2019 gateway review); and the ADHA could also clarify the roles and responsibilities of other government entities in the management of shared risks.

3.2 ADHA is required to establish and maintain an appropriate system of risk oversight and management.[33] As a corporate Commonwealth entity, ADHA is not required to comply with the Commonwealth Risk Management Policy, but 'should review and align their risk management

[33] *Public Governance, Performance and Accountability Act 2013*, section 16.

frameworks and systems with [the] policy as a matter of good practice'.[34] Also, while not mandatory, entities should align their risk management with existing standards and guidance.

3.3 The ADHA Board set the entity risk tolerances, endorsed the strategic risk assessment, and considered risk reporting from the Audit and Risk Committee and the Executive Leadership Team on multiple occasions. The ADHA Board regularly considered risk updates on the My Health Record expansion program. The Board queried risk ratings and mitigation strategies, and requested additional risk reporting and access to risk registers.[35]

3.4 The ADHA risk management framework addressed key elements described in the Commonwealth risk management policy and was supported by:

- an entity-level strategic risk assessment and register, which identified key risks and controls to manage those risks; and
- an 'operational risk register'and program-based risk assessments and registers, including one for the My Health Record expansion program.

3.5 ADHA's entity level strategic risk assessment identified nine strategic risks, of which three were relevant to the My Health Record expansion program and ongoing operation:

- failure to maintain confidentiality, integrity and availability of national infrastructure (i.e. the My Health Record system) within forecast commercial arrangements (risk six);
- failure to provide a clinically safe national infrastructure (risk eight); and
- failure to plan for and deliver the My Health Record expansion program (risk nine).

3.6 For these risks, the documentation identified possible causes or triggers for each risk, current controls and potential treatments, however the specific controls were not linked to specific causes.

3.7 ADHA also maintained a risk management plan and a detailed risk register specific to the My Health Record expansion program. This documentation mapped risks, consequences, controls and residual ratings.

3.8 The 2019 gateway review found that risk management had improved since its 2017 review, but that documentation was not fully mature. It recommended that ADHA 'review and finalise risk management procedures and artefacts in accordance with the agency's framework as set out in the risk management plan'.

Shared risks

3.9 The Commonwealth Risk Management Policy states that 'entities must implement arrangements to understand and contribute to the management of shared risks'.[36] The policy provides several 'tips' for managing shared risks, including: establishing memoranda of understanding with partners to formalise shared risk management; development of shared risk

[34] Department of Finance, *Commonwealth Risk Management Policy,* DoF, [Internet] available from: https://www.finance.gov.au/comcover/risk-management/the-commonwealth-risk-management-policy/, [accessed 21 June 2019].

[35] The ANAO did not access the Board's engagement with financial risk as part of this audit. Specific privacy and cyber security risk management issues are consider later in this report.

[36] Department of Finance, *Commonwealth Risk Management Policy*, 2014, p.16.

registers; educating officials on their responsibilities to identify and manage shared risks; and documenting control owners and governance arrangements for monitoring shared risks.

3.10 ADHA shares My Health Record risks with other system participants, including:

- Services Australia — which manages Medicare data integrity, the myGov platform, and the Healthcare Identifiers Service;
- the National Infrastructure Operator (NIO) — which operates and maintains the My Health Record system and has contractual obligations relating to privacy;
- healthcare provider organisations, medical practitioners, authorised representatives and nominated representatives — who access information from My Health Record;
- software vendors — which develop the clinical information systems that providers use to access and upload information to My Health Record;
- healthcare recipients — whose health and personal information is stored in the My Health Record system; and
- the Information Commissioner — who has additional statutory functions and powers relating to My Health Record, and a Memorandum of Understanding with ADHA.

3.11 ADHA's approach to managing shared risks with government entities included involving those entities in My Health Record governance committees. This includes Commonwealth entities such as Health, Services Australia, Australian Institute of Health and Welfare, and state and territory jurisdictions. The Secretary of Health is a member of the ADHA Board.

3.12 ADHA's risk registers identified some shared risks with other entities. For example:

- Health — which did not maintain its own risk register for My Health Record — is listed in ADHA's registers as owning My Health Record risks relating to legislation and policy, such as policy relating to communicating with 'hard to service' consumer groups; and
- Services Australia was identified as sharing a range of risks related to system access and the provision of Medicare data into My Health Records (such as the creation of records for deceased or ineligible individuals, and risks related to potential data breaches arising from intertwined Medicare records, which are discussed further at paragraph 4.7) — ADHA also has a formal agreement with Services Australia which includes protocols for identifying and managing emerging risks.

3.13 ADHA could further clarify the specific roles and responsibilities of other government entities in managing shared risks by explicitly indicating which risks are shared, with which entities, and who in other entities is responsible for controls implementation. For example, ADHA had identified a risk that improved provider registration may not be ready in time for the opt-out process, as it was dependent on Services Australia delivering its identification solution, but this was not specifically described and managed as a shared risk.

3.14 The My Health Record risks that are shared with non-government entities, such as healthcare providers and software vendors, are particularly relevant to the management of privacy and cyber security risks. These issues are considered in more detail the following sections.

Were privacy risks appropriately managed?

ADHA's management of privacy risks was largely appropriate. Health and ADHA implemented system and consumer access controls. System controls included access requirements for healthcare provider organisations and various consumer controls (including identity verification requirements, the ability to set advanced access controls and the ability to permanently delete records).

The ADHA has not undertaken an end-to-end privacy risk assessment of the ongoing operation of the My Health Record system under the opt-out model. The last privacy specific risk assessment was completed in 2017 and, although ADHA funded the Office of the Australian Information Commissioner to conduct at least four privacy reviews between October 2017 and June 2019, none were completed in that period.

ADHA did not have sufficient assurance arrangements to satisfy itself that all instances of the emergency access did not constitute an interference with privacy. It should therefore review its approach and procedures and for notifying the Information Commissioner of potential contraventions.

3.15 The sensitivity of personal and health information is recognised in Australian privacy law and practice. Relevant privacy risk management standards can be found in:

- the *Public Governance, Performance and Accountability Act 2013*;
- the *Privacy Act 1988*, including the Australian Privacy Principles;
- the *My Health Records Act 2012* and related legislation;
- the *Healthcare Identifiers Act 2010*;
- state and territory laws regulating privacy and health information; and
- professional standards and ethical codes of practice for healthcare providers.

3.16 The ADHA Board set the privacy risk appetite for the entity as 'limited' in 2017 and reinforced this in August 2018.[37] ADHA's Risk Management Strategy identified privacy risk as a specialist risk type requiring 'specific additional risk management and assessment policies, guidelines and reporting', as well as targeted risk assessments, annual reporting, and summary reporting in the risk register.

Privacy risk assessment

3.17 Privacy risks for My Health Record were assessed through activities including commissioned Privacy Impact Assessments (PIAs) and other assessments.

3.18 Ten reports were commissioned to assess privacy risks of My Health Record between December 2011 and July 2017, focussing on various aspects of the system design and operation (outlined at Appendix 2). The evaluation of the participation trials also considered privacy risks. The earlier reports (2011–2016) informed the development of the 'opt-in' Personally Controlled Electronic Health Records (PCEHR) system, design of the participation trials, and technical

[37] 'Limited' was the lowest of three risk appetite levels defined by the Board in 2017. The lowest level was revised to 'zero' in 2018. In both cases, privacy risks were identified as being at the lowest appetite level.

processes. The most recent assessments examined specific issues related to the transition to opt-out:

- in December 2016, a PIA assessed the bulk transfer of records to the National Infrastructure Operator for record creation as part of the opt-out process; and
- in July 2017, a PIA examined privacy risks of the opt-out process and made 11 recommendations relating to opt-out communications and the bulk registration of records after the opt-out period.

3.19 Recommendations from these assessments were addressed as part of the My Health Record expansion program.

3.20 A security review of the system in 2016 also identified risks with variable healthcare provider awareness of privacy and security (see paragraph 3.58).

Assessments by the Office of the Australian Information Commissioner

3.21 Between 2011 and 2017, the OAIC undertook 14 privacy assessments in relation to the My Health Record system and the Healthcare Identifiers Service.[38]

3.22 ADHA entered into a Memorandum of Understanding with the OAIC in 2017, covering the period 1 October 2017 to 30 June 2019. Under this agreement, ADHA provided funding of $3.6 million to OAIC which included a minimum of four and up to six assessments to be conducted in relation to My Health Record and the Healthcare Identifiers Service. No assessments were completed during this period.[39]

3.23 Despite the failure to complete any privacy assessments under the 2017-2019 Memorandum of Understanding before the nominal end date of 30 June 2019, ADHA entered into a new agreement with the OAIC on 26 June 2019 for an additional $2.1 million. This agreement is to continue the OAIC's regulatory and complaints management functions, and to conduct at least two assessments relating to My Health Record and the Healthcare Identifiers Service.

Senate committee inquiries

3.24 Two Senate committee inquiries considered privacy risks in the My Health Record system (as discussed at paragraphs 1.17 and 1.18). The government had not tabled a response to either report by October 2019. Of the 14 recommendations relating to privacy, the ANAO observed that ten were implemented, one partly implemented, and three not implemented (see Appendix 3).

[38] OAIC reports are available at https://www.oaic.gov.au/privacy/privacy-assessments [accessed 19 November 2019].

[39] The Office of the Information Commissioner stated to the ANAO in November 2019 that document review and fieldwork for four of these assessments had been completed and that assessment reports were expected to be finalised in the 2019–20 financial year.

Comprehensiveness of assessments

3.25 The Commonwealth Risk Management Policy states that 'each entity must review its risks, its risk management framework and the application of its risk management practices on a regular basis'.[40]

3.26 The last privacy specific risk assessment was completed in 2017. These focused on either specific elements of the system's operation or management aspects of the opt-out implementation process. Now that My Health Record is operating as an opt-out model – with 90 per cent of Australians having a record – a comprehensive, end-to-end privacy risk assessment on the ongoing operation of the My Health Record system should be considered.

Recommendation no.1

3.27 ADHA conduct an end-to-end privacy risk assessment of the operation of the My Health Record system under the opt-out model, including shared risks and mitigation controls, and incorporate the results of this assessment into the risk management framework for the My Health Record system.

Australian Digital Health Agency response: *Agreed.*

3.28 *The Agency will work with public and private sector healthcare providers, professional associations, consumer groups and medical indemnity insurers on an overarching privacy risk assessment, and incorporate results into the risk management plan for My Health Record.*

Control, treatment and monitoring of privacy risks

3.29 ADHA implemented various processes to control, treat and monitor privacy risks:

- general preventive controls;
- system access controls;
- consumer access controls;
- the ability to cancel and delete records; and
- monitoring of the 'emergency access' override function.

General preventive controls

3.30 ADHA stated to the ANAO that external environmental controls contribute to reduced likelihood of privacy risks presented by the My Health Record — including medical indemnity insurance requirements, professional accreditation standards, practice accreditation standards, and reputational risk for providers involved in data breaches.

3.31 There are statutory controls within the My Health Record legislative framework. For example, in order to be eligible and remain eligible for registration, healthcare provider

[40] Department of Finance, *Commonwealth Risk Management Policy,* DoF, [Internet] available from: https://www.finance.gov.au/comcover/risk-management/the-commonwealth-risk-management-policy/, [accessed 21 June 2019].

organisations must have policies governing access to the My Health Record system and reasonable user account management practices.[41]

3.32 The legislative framework contains penalties for unauthorised use, collection or disclosure of information in a My Health Record, or other misuse of information in a My Health Record.[42] Since 10 December 2018, this has included unauthorised use of information in a healthcare recipient's record for prohibited purposes such as: underwriting or determining whether to enter into a contract of insurance that covers the healthcare recipient; determining whether a contract of insurance covers the healthcare recipient in relation to a particular event; and an employer employing, or continuing or ceasing to employ, the healthcare recipient.[43]

3.33 Entities must notify ADHA or the OAIC of actual or potential contraventions, events or circumstances relating to a My Health Record or the My Health Record system that directly involved, may have involved or may involve the entity.[44] In 2017–18, the OAIC received 28 notifications. Of these, 26 notifications were from Services Australia (17 related to intertwined Medicare records, and 9 related to fraudulent Medicare claims – these types of breaches are discussed further at paragraph 4.8); and two were from ADHA (one was unauthorised access to a My Health Record related to a Medicare fraud, and one was accidental access to an incorrect record). In total these notifications affected 65 individuals.

System access controls

3.34 The My Health Record system incorporated system access controls, including:

- identity verification requirements for healthcare recipients through the MyGov portal;
- unique Healthcare Identifiers for healthcare recipients, healthcare provider organisations and individual healthcare providers for accessing the system (see Box 2)[45]; and
- access requirements for healthcare provider organisations accessing the My Health Record system through their clinical information systems.

Box 2: Healthcare provider access to the My Health Record system

Healthcare providers access the My Health Record system through the National Provider Portal (NPP), which provides view only access, or a clinical information system registered with ADHA.

To access a My Health Record through the NPP, a healthcare provider must:

- enter an assigned Healthcare Provider Identifier-Individual (HPI-I) linked to a Healthcare Provider Identifier- Organisation (HPI-O) and authorised to access the portal; and
- enter the name, Medicare card number (or IHI or DVA number), sex and date of birth of the individual whose My Health Record they are trying to access.

[41] *My Health Records Rule 2016*, Part 5 Divisions 3 and 4 set out ongoing eligibility requirements for registration.

[42] *My Health Records Act 2012*, Part 4.

[43] *My Health Records Amendment (Strengthening Privacy) Act 2018*.

[44] *My Health Records Act 2012*, section 75. Entities include the ADHA as System Operator; registered healthcare provider organisations; registered repository operators (such as Medicare); registered portal operator (such as MyGov); or a registered contracted service provider.

[45] Services Australia operates the Healthcare Identifiers Service and issues the unique identifiers.

To access a My Health Record through a clinical information system, a provider must:

- be involved in the healthcare of the healthcare recipient;
- have a secure, encrypted connection to the My Health Record system;
- be authorised to access the clinical information system by a healthcare provider organisation; and
- access the My Health Record through the healthcare recipient's patient record on the local clinical information system.

Source: ANAO based on ADHA documentation.

Consumer controls

3.35 The My Health Record system included consumer preventive controls through 'default' and 'advanced' access settings (see Box 3). The 'default access setting' permits all registered healthcare provider organisations involved in the care of a healthcare recipient to access that recipient's record and to upload documents. Healthcare recipients may also activate 'advanced access settings' to restrict access to their information.

Box 3: Default and advanced access settings

Under 'default' access settings, all healthcare recipients may:

- view an access history to see which healthcare provider organisations or nominated representatives have accessed their record;
- remove or hide a document; and
- cancel their record and have it permanently deleted — if they subsequently decide to 'opt in' again, the new record will not include previously deleted documents.

Under 'advanced' access settings, healthcare recipients may also choose to:

- set a Record Access Code (RAC) to restrict which healthcare provider organisations can see their information, including those that have previously accessed their information;
- adjust the level of access healthcare provider organisations have (view-only or write/upload access);
- classify certain documents as restricted and set a Limited Document Access Code (LDAC) so only specified healthcare provider organisations can view the documents;
- set up an email or SMS notification for whenever a new healthcare provider organisation accesses their record, or if it is accessed in an emergency; and
- choose not to share their de-identified data for secondary use research.

Healthcare provider organisations can override advanced access settings in an emergency.

ADHA also has procedures for hiding address details or removing an authorised representative (e.g. a parent of a child) in cases of family and domestic violence. Individuals may also use a pseudonym for their My Health Record.

Source: ANAO, adapted from ADHA documentation.

3.36 As at 30 June 2019, a Record Access Code had been set for 27,215 records – 0.1 per cent of all records – and a Limited Document Access Code had been set for 3,862 documents in the system.

3.37 Consumers have direct access to their health information in the system and may identify and seek corrections to errors in their records.[46] They can view access logs and report potential interference with privacy. ADHA documented protocols and procedures to follow-up access complaints.

Permanent deletion of records

3.38 Healthcare recipients can cancel their My Health Record registration. Since January 2019, they can also request permanent deletion of clinical information held in their records (the deletion process was applied retrospectively to cancellation requests prior to January 2019).[47] ADHA had detailed procedures for the management of requests, and this was supported by operational monitoring. Permanent deletion occurs through an automated two-step process, starting when a healthcare recipient requests record cancellation:

- an initial immediate cancellation – this stops anyone from accessing the record, including any data or clinical documents stored on the record from that point onwards; and
- the subsequent deletion – this occurs within the next 48 hours, and deletes all clinical information held in the record from the various system data stores. [48]

3.39 Healthcare recipients who request cancellation online receive a success notification on-screen advising them their record is cancelled and will be deleted. Healthcare recipients may also choose to receive an SMS or email confirmation. Healthcare recipients' Individual Healthcare Identifiers are retained in the system when records are deleted, and a note is made against the identifier that the deletion was successful.

3.40 The information is also removed from system back-ups, but this may not occur immediately: ADHA stated that 'deleted records are removed from the backup when a new backup is created during regular backup cycle'.[49]

3.41 The ANAO reviewed the documentation that supported the design and build of the permanent deletion system functionality. While this review was not technical in nature and did not involve system testing, the ANAO assessed that the documents reflected a design that was consistent with the legal requirement to permanently delete clinical data and documents.[50]

[46] Healthcare recipient access to records in the My Health Record system gives persistent and practical effect to Australian Privacy Principle 12 (access to personal information) and Australian Privacy Principle 13 (correction of personal information).

[47] *My Health Records Act 2012*, section 51. Deletion was retrospectively applied to all previous cancellation requests.

[48] The exception is for healthcare recipients with multiple authorised representatives: here ADHA 60 days for representatives to review to confirm the cancellation request is appropriate.

[49] This does not include information that may be retained under legislation (such as the name and healthcare identifier of the healthcare recipient, the name and healthcare identifier of the person who requested cancellation, and the date), nor does it include system information about the deletion process.

[50] The ANAO did not conduct testing to verify this process.

Emergency access function

3.42 Registered healthcare provider organisations and other system participants[51] may use an ‘emergency access’ override function to access a My Health Record in circumstances involving a serious threat to an individual’s life, health or safety, or a serious threat to public health or public safety. This function overrides any advanced access settings set by healthcare recipients. Use of this function outside of the limited statutory circumstances could constitute an interference with privacy. ADHA assessed that use of this function had a ‘very high’ inherent privacy risk.

3.43 System participants must advise ADHA of the circumstances of emergency access, and must notify ADHA and the Information Commissioner as soon as practicable after becoming aware that a contravention of the Act has or may have occurred.[52] ADHA monitors use of the emergency access function. Monthly use of the function increased from 80 instances in July 2018 – prior to the transition to an opt-out model – to 205 instances in March 2019, representing approximately 0.1 per cent of instances of system access. In only 8.2 per cent of those instances was the emergency access function used to access records which had advanced access controls set (in other words, in only 8.2 per cent of instances was it used as intended): this suggests a need for further healthcare provider training on the emergency access function.

3.44 ADHA documented a procedure for monitoring emergency access, but not next steps for receipt, assessment or monitoring of responses. ADHA sought written responses from healthcare provider organisations in relation to each instance of emergency access, and maintained detailed records and analysis of provider responses. In a number of instances, ADHA did not receive a response from specific healthcare provider organisations. In these cases ADHA could not satisfy itself that the circumstances of the emergency access did not constitute an interference with privacy. In other instances, some of the responses indicated a potential contravention of the Act. To date, ADHA has not notified the Information Commissioner of any of these instances, and nor have the healthcare provider organisations.

[51] *My Health Records Act 2012*, section 5 defines ‘participant in the My Health Record system’ to mean the System Operator (ADHA); a registered healthcare provider organisation; the operator of the National Repositories Service; a registered repository operator; a registered portal operator; and a registered contracted service provider, so far as the contracted service provider provides services to a registered healthcare provider.

[52] *My Health Records Act 2012*, section 64 and section 75.

Recommendation no.2

3.45 ADHA, with the Department of Health and in consultation with the Information Commissioner, should review the adequacy of its approach and procedures for monitoring use of the emergency access function and notifying the Information Commissioner of potential and actual contraventions.

Australian Digital Health Agency response: *Agreed.*

3.46 *The Agency will work with the Department of Health and OAIC on the use of the emergency access function and monitoring by the Agency, and compliance with our obligations for notifications.*

Department of Health response: *Agreed.*

3.47 *The Department of Health (the Department) is committed to protecting the privacy and security of people's health information. The department is dedicated to working with, and supporting, the Agency and the Information Commissioner to review the approach and procedures for monitoring the emergency access function within the My Health Record system to continue to ensure people's health information remains protected.*

Were there appropriate systems of cyber security risk management and oversight?

ADHA had largely appropriate systems to manage cyber security risks to the core infrastructure of the My Health Record system, except its management of the broader shared cyber security risks were not appropriate and its oversight processes should be improved. ADHA managed risks to the core infrastructure through: establishing a Digital Health Cyber Security Centre; undertaking a series of dedicated cyber security assessments; and implementing the 'Essential Eight' cyber security mitigation strategies and decreasing the number of ISM cyber security controls not implemented. ADHA's approach to managing shared cyber security risks in the broader system was not appropriate. This should be improved by:

- developing an assurance framework for third party software connecting to the My Health Record system in accordance with the Information Security Manual; and
- developing a strategy to monitor compliance with legislated security requirements by registered healthcare provider organisations.

Cyber security risk oversight by the AHDA Board and its Privacy and Security Advisory Committee could also be strengthened. The ADHA Board received cyber security briefings on only four occasions between July 2016 and February 2019, and did not approve the updated 2019–2023 Cyber Security Centre Strategic Plan (finalised by the ADHA executive in November 2018). The role of the Privacy and Security Advisory Committee in cyber security was also not clear.

3.48 To examine whether there were appropriate systems to oversee and manage My Health Record cyber security risks, the ANAO considered:

- cyber security risk context and standards;
- core infrastructure cyber security risk management;

- shared cyber security risk; and
- oversight of cyber security risks.

3.49 Analysis is based on a review of ADHA's documentation and management frameworks. The ANAO did not test the technical effectiveness of cyber security controls as part of this audit.

Cyber security risk context and standards

3.50 The healthcare sector in Australia and overseas faces cyber security risks, such as phishing (compromised credentials), hacking and malware. International examples include a 2017 ransomware incident on the UK's National Health Service[53], and a 2018 cyberattack on SingHealth's IT system in Singapore.[54]

3.51 In Australia, evidence shows that:

- not all healthcare provider organisations achieve minimum cyber security levels[55];
- in 2018, the private health service provider sector reported the most notifiable data breaches of any industry sector; and
- more than 40 per cent of data breaches from the private health service provider sector notifications to the OAIC in 2018 were due to malicious or criminal attacks, almost half of which were cyber incidents.[56]

3.52 In early 2016, ADHA assessed the cyber security risk context for My Health Record, and identified 'nation states and criminal actors as the greatest threat to the My Health Record system, with hacktivists and trusted insiders posing a medium threat and cyber terrorists posing a low threat'. ADHA assessed that in addition to denial of service attacks, sensitive information holdings 'could be used for identity theft, leverage or blackmail', and 'manipulation of the system or the information contained within the system could be used to attack the nation's health system as a whole, or to cause physical harm to an individual by changing the content of their health record'.

3.53 In 2017, the ADHA Board set a 'limited' risk appetite and 'low' risk tolerance for cyber security-related risks. The ADHA established the Digital Health Cyber Security Centre (CSC) to 'strengthen the security of our national digital health systems and services; and to promote increased security awareness and maturity across the digital health sector'.[57]

[53] Australian Cyber Security Centre, *Ransomware campaign impacting organisations globally* [Internet], https://www.cyber.gov.au/news/ransomware-campaign-impacting-organisations-globally, 13 May 2017 [accessed 19 November 2019].

[54] Committee of Inquiry, *Public Report into the Cyber Attack on Singapore Health Services,* 10 January 2019, https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2019/1/public-report-of-the-coi; Ministry of Health (Singapore) [accessed 19 November 2019].

[55] Several state and territory auditors-general have reported on health sector vulnerability to cyberattacks.

[56] For notifiable data breach reporting, see the Office of the Australian Information Commissioner, *Notifiable Data Breaches Quarterly Statistics Report series* [Internet], https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics-reports/ [accessed 19 November 2019].

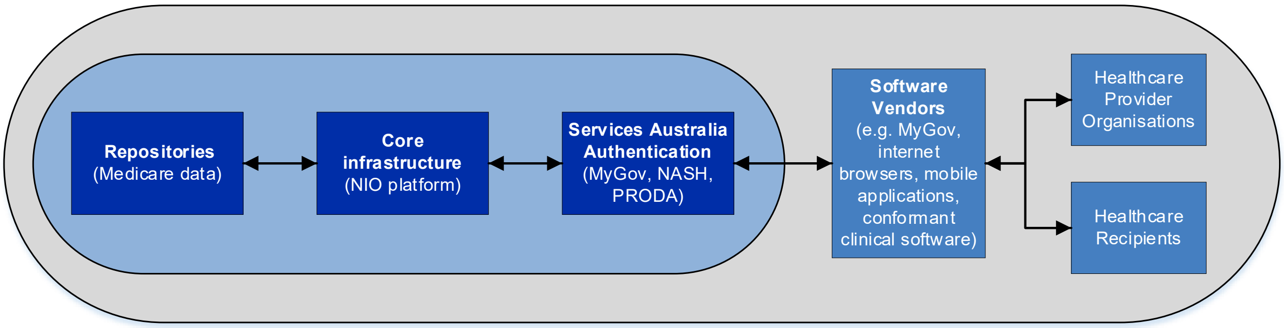
[57] Australian Digital Health Agency, *Digital Health Cyber Security Centre*, https://www.digitalhealth.gov.au/about-the-agency/digital-health-cyber-security-centre [accessed 19 November 2019].

3.54 Under legislation the ADHA is required to: establish and maintain an appropriate system of risk oversight and management; maintain the confidentiality, integrity and availability of all official information; and exercise effective governance of information resources. ADHA also applied the Australian Government Protective Security Policy Framework (PSPF) core and supporting requirements, and the Information Security Manual (ISM), as mandatory requirements for the My Health Record system.[58]

3.55 As with privacy risks, ADHA shares cyber security risks with other participants, including:

- the NIO and subcontractors – provide the core infrastructure for the My Health Record system, and have legislative and contractual security obligations;
- Services Australia – secures the data repositories and myGov portal, provides healthcare provider authentication through the National Authentication Service for Health (NASH) public key infrastructure (PKI) certificates and the National Provider Portal[59], and monitors the Healthcare Identifiers Service for anomalous transactions;
- software vendors – are responsible for the security of software used to access the My Health Record system, including clinical software used by healthcare providers and mobile applications used by healthcare recipients;
- healthcare provider organisations and their contracted service providers – have access to multiple records by design, and are responsible for their information management and cyber security practices; and
- individual healthcare recipients – are responsible for the security of the passwords, devices and connections they use to access their My Health Record, either through myGov or third party mobile applications.

Figure 3.1: Shared risks in the My Health Record system


Repositories (Medicare data)
Core infrastructure (NIO platform)
Services Australia Authentication (MyGov, NASH, PRODA)
Software Vendors (e.g. MyGov, internet browsers, mobile applications, conformant clinical software)
Healthcare Provider Organisations
Healthcare Recipients

Source: ANAO, adapted from ADHA, National Digital Health Cyber Security Centre Strategic Plan 2016-2019.

[58] The Council of Australian Governments amended the *Intergovernmental Agreement on National Digital Health* in March 2017 to acknowledge that ADHA will comply with the PSPF and ISM: https://www.coag.gov.au/sites/default/files/agreements/digital-health-iga-signed-2.pdf. These standards are typically only better practice rather than mandatory for corporate Commonwealth entities such as ADHA.

[59] Healthcare providers and supporting organisations use NASH to securely access and share health information, including on the My Health Record system. NASH is due to be replaced by Provider Digital Access (PRODA), currently used for the National Provider Portal (NPP), consistent with the deadline for new security standards set out by the Australian Signals Directorate that require people and organisations that transact digitally with Government to transfer from PKI to PRODA by 2022. The NPP is an interface through which healthcare providers can access the My Health Record system without the need for conformant clinical software.

Core infrastructure cyber security risk management

3.56 The ICT platform and associated processes that comprise the central My Health Record system are referred to here as the 'core infrastructure'. Core infrastructure consists of the software, equipment and interfaces that are operated by the National Infrastructure Operator on behalf of ADHA as the System Operator. Other ICT systems connect to the core infrastructure to make My Health Record function as intended—such as the authentication services, data repositories, and external clinical information systems software (as shown in Figure 3.1). The ANAO considered core infrastructure risk management, as well as the management of shared risks to cyber security.

3.57 The PSPF accreditation framework requires that entities assess, certify and accredit ICT systems in accordance with the ISM.[60] This involves:

- assessment – to review the system architecture and documentation and examine the effectiveness of security measures;
- certification – the entity 'certifies' that security measures have been implemented and are operating effectively to ensure the system's integrity and confidentiality; and
- accreditation – the entity accepts any residual security risk to the system and documents an approval for the system to operate.[61]

3.58 The My Health Record system underwent five information security assessments between 2012 and 2017. These were conducted by an external Information Security Registered Assessors Programme (IRAP) registered assessor. The most recent assessment was completed in 2017 in the lead-up to the opt-out period. The next assessment is due by late 2020.

3.59 ADHA should improve its mechanisms for tracking the IRAP recommendations:

- the 2017 assessment found that 11 of 31 recommendations from the previous 2015 IRAP assessment were still 'open' and not implemented;
- in 2018, a security risk management plan incorporated reference to some but not all recommendations from the 2017 IRAP assessment, and did not indicate whether these recommendations had been implemented;
- from June 2019, the NIO prepared a My Health Record security risk register that documented 74 risks in a comprehensive risk framework, but did not document any proposed risk treatments, controls, or assessment of the effectiveness of controls — including for the 15 'high' and five 'very high' risks.

3.60 Following these IRAP security assessments, the system was certified and accredited by Health in 2013 and 2016, and by ADHA in 2018. Each time the system was accredited by a senior executive below the accountable authority, which is permissible under the PSPF. ADHA could consider elevating future accreditation decisions to the accountable authority (the ADHA Board).

[60] Australian Government, *Core Requirement 11 Robust ICT systems* [Internet], Protective Security Policy Framework, available at https://www.protectivesecurity.gov.au/information/Pages/default.aspx [accessed 19 November 2019].

[61] An ICT system can be accredited even though a security assessment identifies non-compliance with ISM controls, as some ISM controls are non-mandatory, an entity can rely on compensating controls at certification, and the accrediting authority accepts any residual risk of non-compliance at accreditation.

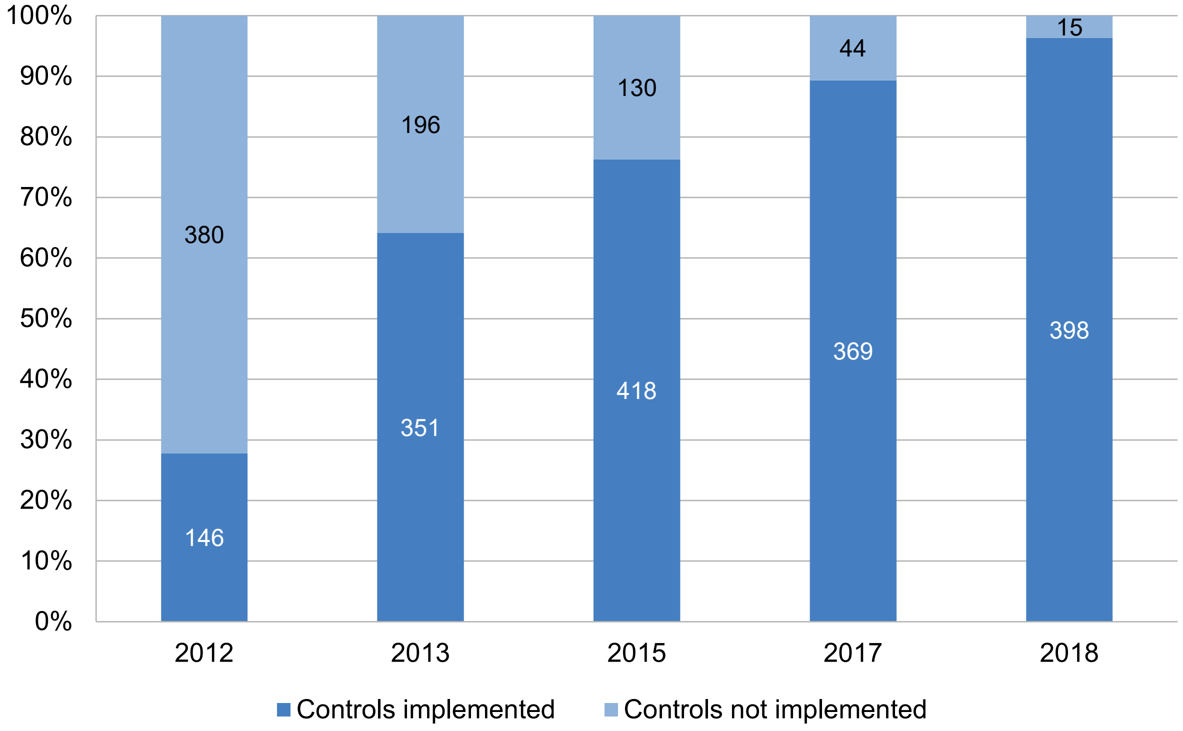
3.61 In addition to the IRAP assessments, a number of other risk assessments and end-to-end security reviews were commissioned. Reviews in 2015 and 2016 found that threats to core infrastructure were being managed through relatively strong security controls and that healthcare provider security remained a challenge.

Information Security Manual controls

3.62 The most recent IRAP security assessment in 2017 found that for the My Health Record core infrastructure ADHA had implemented the 'Top Four'[62] and 'Essential Eight'[63] cyber security mitigation strategies recommended by the Australian Cyber Security Centre. In addition the PSPF framework requires that 'residual security risks to the system and information have been recognised and accepted' in accordance with the ISM.[64]

3.63 Further work is required to implement all ISM security controls (illustrated in Figure 3.2). Health and ADHA reported internally that the number of ISM cyber security controls not implemented over core infrastructure decreased over time. This was confirmed by the IRAP assessments.

Figure 3.2: Reported ISM cyber security controls implemented over time



Source: ANAO analysis of information from the Department of Health and Australian Digital Health Agency. The total number of controls varies between years due to changes in ISM requirements.

[62] PSPF Chapter 10 *Safeguarding information from cyber threats*, has a core requirement that entities implement the Top Four strategies to mitigate cyber security incidents.

[63] PSPF Chapter 10 *Safeguarding information from cyber threats* states that the Attorney-General's Department strongly recommends entities implement the Australian Cyber Security Centre's Essential Eight strategies to mitigate cyber threats. The Essential Eight cyber security controls are consistent with the ISM and include the mandatory Top Four.

[64] PSPF Chapter 11 *Robust ICT systems*, supporting requirement 2.

3.64 ADHA cyber security risk management arrangements with the NIO for core infrastructure are based on clearly defined roles and responsibilities documented in the NIO contract. While the contract required the NIO to comply with the PSPF and the ISM, this did not initially result in core infrastructure that implemented all applicable ISM cyber security controls. Additional funding was provided to the NIO to implement security improvements and increase the number of ISM cyber security controls for the core infrastructure.

Monitoring and other security activities

3.65 The CSC includes a Security Operations Centre, which monitors the My Health Record system using security incident and event management software, and provides an incident response management capability. ADHA stated to the ANAO that 'the My Health Record system has not been the subject of any actual malicious cyber activity, events or incidents'.

3.66 ADHA also documented cyber security risks in corporate risk management plans. In 2018, the CSC reported that three residual risks remained above tolerance and were being actively managed:

- multiple health records are accessed, modified or made unavailable without authorisation due to vulnerabilities or bugs from development in the My Health Record system;
- multiple health records are accessed, modified or made unavailable without authorisation due to compromise of a participating healthcare organisation or their contracted service provider (including unauthorised access by a member of staff); and
- the My Health Record system is not available for individuals or healthcare providers due to a malicious denial of service attack against the hosting infrastructure.

3.67 Another security measure relates to the storage of information in Australia. The NIO must notify ADHA if the NIO, or subcontractor or personnel, is subject to an order made under the 'law of a foreign country to disclose or transfer data it holds in relation to a My Health Record to a foreign country or to any entity outside Australia…if permitted by such law'. Legislative and contractual requirements can only be partially effective controls against this risk, which can also be mitigated in the selection of contractor. Future procurement processes for core infrastructure and data storage should consider the risk that an external contracted service provider or subcontractor is subject to direction from a foreign government that contravenes Australian law and places sensitive information at risk.

3.68 Regarding information classification, while ADHA's approach is consistent with the PSPF, the classification is not displayed or documented on the user interface for healthcare providers. ADHA could consider amending the user interface and key documents to ensure the classification — or an equivalent statement that the information is sensitive — is displayed on the user interface and documents viewed, extracted or printed from the My Health Record system.

3.69 The ADHA maintains 'hot' and 'warm' sites, which provide a failover in case of technical failure at one site. The 2017 security assessment recommended that ADHA review the geographic location of data centres to provide better resilience against geographically focussed attacks and incidents.

Shared cyber security risks from the broader My Health Record system

3.70 ADHA assessed shared cyber security risks potentially posing 'high' to 'very high' residual risk to the My Health Record system.

3.71 ADHA conducted assessments of shared cyber security risks but did not appear to focus on potential consequences to vendors, healthcare providers and healthcare recipients. Shared risk assessments considered all key stakeholder groups — the NIO, Services Australia, software and mobile application vendors, healthcare providers and healthcare recipients — however primarily focused on consequences to the ADHA itself and the in-house technical ICT controls and treatments protecting core infrastructure.

Software vendor shared risk

3.72 ADHA's end-to-end security review in 2016 recommended accreditation for contracted service providers of healthcare provider organisations, such as software vendors of clinical information systems. ADHA rejected this recommendation on the basis that it 'presents several challenges' including the additional burden to vendors and potential for reputational damage.

3.73 The IRAP security assessment in 2017 stated that ISM compliance should be considered a minimum acceptable standard for the My Health Record system — as an ICT environment with service-oriented architecture and extensive access by third party software. The IRAP assessment also stated that software products and services used by healthcare providers and recipients, including mobile applications, are an area of risk that needs to be carefully monitored as part of the supply chain managed by ADHA as the System Operator.

3.74 ADHA did not assess, certify or accredit the ISM compliance of third party software and systems connected to the My Health Record system. This included clinical software that gives healthcare providers access to multiple health records, and mobile applications for healthcare recipients. Instead, software vendors must complete a Conformance Vendor Declaration Form and a 'deed poll' that warrants their conformance testing against requirements set by ADHA. Mobile application vendors must sign a Portal Operator Registration Agreement that details their responsibilities and obligations.

3.75 The decision to not assess, certify or accredit the ISM compliance of third party software and systems — as required by the PSPF — limited ADHA's assurance over the cyber security risks of the My Health Record system.[65] An ISM assessment, certification and accreditation approach would provide a rigorous system for ADHA to understand and manage cyber security risks from third party software, but any assurance process must be balanced against disincentives to register and use the system.

[65] PSPF Chapter 10 *Safeguarding information from cyber threats*, supporting requirement 5 ('entities must not expose the public to unnecessary cyber risks when they transact online with government'); PSPF Chapter 11 *Robust ICT systems*, core requirement 'each entity must have in place security measures during all stages of ICT systems development. This includes certifying and accrediting ICT systems in accordance with the Information Security Manual when implemented into the operational environment'.

Recommendation no.3

3.76 ADHA develop an assurance framework for third party software connecting to the My Health Record system — including clinical software and mobile applications — in accordance with the Information Security Manual.

Australian Digital Health Agency response: *Agreed.*

3.77 *An assurance framework exists for systems (including clinical software and mobile applications) connecting to the Healthcare Identifiers Service and the My Health Record system, including processes to confirm conformance. The Agency will review the standards that apply to these systems, and alignment with the Information Security Manual. We will work with industry to update the assurance framework as required.*

Healthcare provider organisation shared risk

3.78 The ADHA shared risk assessments identified cyber security awareness and practices of healthcare provider organisations as a key potential risk. The CSC conducts security and compliance 'outreach' activities to mitigate these risks by raising awareness of good cyber security practice. For example, it published cyber security information and awareness products, including a guide for procurement of secure information technology and other security and privacy guidance.[66] ADHA could consider doing more in this area.

3.79 If a security threat is detected on a provider's system (such as malicious software), ADHA can suspend access to the My Health Record system until that user mitigates the threat. The consequence of temporary suspension of access may be limited for a small healthcare provider, but potentially extensive for a larger provider such as a major hospital or pharmacy. ADHA could develop procedures to inform and assist end users to respond to the impact of cyber security incidents, and test those procedures through crisis simulation exercises.

3.80 Entities such as healthcare provider organisations and contracted service providers must comply with mandatory legislated security requirements in order to be eligible, and remain eligible, for registration.[67] As the System Operator, ADHA should not register an ineligible entity, and may consider revoking registration of an entity that does not remain eligible.[68] Despite clear statutory functions and powers to register and deregister entities, ADHA stated to the ANAO that 'it is unclear that the Agency has a mandate to undertake such monitoring and assurance activities'. Legislative requirements are only effective risk controls when enforced. ADHA conducted limited compliance monitoring to ensure registered healthcare providers met legislated security requirements. ADHA stated to the ANAO that:

[66] These products are available from the Australian Digital Health Agency, *Digital Health Cyber Security Centre*, https://www.digitalhealth.gov.au/about-the-agency/digital-health-cyber-security-centre [accessed 19 November 2019].

[67] *My Health Records Act 2012*, section 43 and *My Health Records Rule 2016*, Part 5 Divisions 3 and 4.

[68] The System Operator may decide to cancel or suspend the registration of a healthcare provider organisation or contracted service provider if the System Operator is no longer satisfied that the entity is eligible to be registered: *My Health Records Act 2012*, section 51.

> Through our engagement with clinicians, they have told us that security and compliance controls can make the provision of healthcare unworkable. This can increase clinical safety risks and place additional pressure on the health workforce which is often already strained.

3.81 The risk that multiple health records are accessed, modified or made unavailable without authorisation due to compromise of a participating healthcare organisation or their contracted service provider remains a shared risk above ADHA's residual risk tolerance. Quality reviews undertaken by ADHA of a very small sample of general practices against the requirement to have a security policy found that this requirement was only fully met by 32 per cent of survey recipients.

Recommendation no.4

3.82 ADHA develop, implement and regularly report on a strategy to monitor compliance with mandatory legislated security requirements by registered healthcare provider organisations and contracted service providers.

Australian Digital Health Agency response: *Agreed.*

3.83 *The Agency will develop, implement and regularly report on a compliance program that monitors adherence to security requirements.*

Oversight of cyber security risks

3.84 The ADHA Board noted dedicated cyber security briefings on four occasions between July 2016 and February 2019. This included noting the 2016–2019 Cyber Security Centre Strategic Plan and its 12 Key Performance Indicators (KPI) on 21 February 2017. Progress reporting against these KPI has not been provided back to the Board.

3.85 One of the ADHA Board's advisory committees is the Privacy and Security Advisory Committee (PSAC). The PSAC Charter states that it will 'monitor privacy and security issues in relation to digital health systems', 'provide advice and recommendations to the Board in relation to standards (including compliance with standards) relating to privacy and security' and 'provide advice to the Board about the privacy and security issues encountered by users of digital health systems'.

3.86 It was not clear that the PSAC provided advice or recommendations to the ADHA Board, despite meeting minutes recording that the PSAC noted regular briefings from ADHA on cyber security. As part of these meetings PSAC also noted the 2016–2019 Cyber Security Centre Strategic Plan on 23 March 2017, and reviewed the underpinning work plans supporting the strategy on 1 August 2018. Progress reporting against these KPI has not been provided back to PSAC. The ADHA updated the Cyber Security Centre Strategic Plan for 2019–2023 on 14 November 2018. The meeting minutes to April 2019 do not show that the updated Strategy was considered by the PSAC or the ADHA Board.

4. Monitoring and evaluation

Areas examined

This chapter examines the appropriateness of monitoring and evaluation for the My Health Record system.

Conclusion

The monitoring and evaluation arrangements for My Health Record are largely appropriate. There are appropriate mechanisms to improve the quality of information entered into the system. Some benefits measurement activities are underway, but they are not yet organised in a research delivery and evaluation plan setting out milestones, timeframes and sequencing of activities over forward years.

Areas for improvement

The ANAO recommended that ADHA develop a forward research delivery/evaluation plan for My Health Record, expanding on the benefits realisation work undertaken to date.

4.1 To examine the appropriateness of monitoring and evaluation for the My Health Record system, the ANAO considered:

- whether mechanisms have been put into place to improve the quality of data — because the quality of information entered into the system is critical to increasing the use of the system by healthcare providers, and therefore to the realisation of intended benefits; and
- whether there are arrangements to monitor, evaluate and report on the realisation of the intended benefits — because the timeframe for benefits realisation is relatively long, it is important that arrangements in place to collect and evaluation relevant performance information over time.

4.2 Analysis in this section is based on a review of documentary evidence.

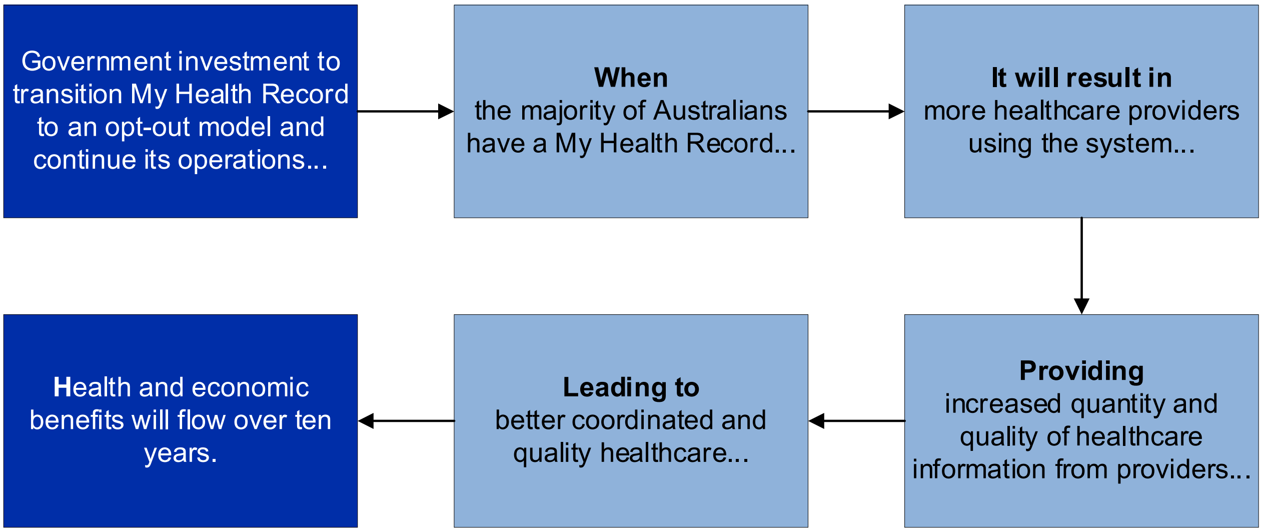
Are there appropriate mechanisms to improve the quality of information entered into the My Health Record system?

There are appropriate mechanisms to improve the quality of information entered into the system, such as: procedures to detect and correct administrative data errors; processes to promote consistency in how information is entered into the system; and data quality education and training activities. Work to monitor and improve data quality will need to continue as use of the system increases, especially if different types of users, who may not have accessed awareness and education activities, increase their participation over the coming years (such as medical specialists, allied health and aged care providers).

4.3 Data quality is critical to realising the potential benefits from My Health Record, and the *My Health Records Act 2012* established an objective to 'improve the quality of health information'. While there is no baseline or benchmark against which 'improvement' is measured, the theory of change described in the 2017 business case suggested that increasing the availability and sharing of clinical information in the My Health Record system was both an intermediate success indicator for the system, and a foundation for realising its intended longer-term benefits.

4.4 As summarised in Figure 4.1, the business case stated that increasing the number of individual records would lead to increased use of the system by healthcare providers, resulting in increased availability and sharing of clinical information, which would promote better health care. Implicit in this business case is that the available information is of sufficient quality that providers change their behaviours, and that such behavioural change will generate a range of benefits (which are discussed at paragraph 4.19).

Figure 4.1: Theory of change for the My Health Record opt-out benefits case



Government investment to transition My Health Record to an opt-out model and continue its operations...

When the majority of Australians have a My Health Record...

It will result in more healthcare providers using the system...

Providing increased quantity and quality of healthcare information from providers...

Leading to better coordinated and quality healthcare...

Health and economic benefits will flow over ten years.

Source: ANAO analysis of 2017 business case

4.5 To assess 'data quality', the ANAO considered three broad elements:

- information provided to My Health Record from external repositories;
- information directly entered by healthcare providers (shared health summaries, event summaries, discharge summaries, prescription and dispense records); and
- other activities intended to promote improved data quality.[69]

Data quality: repository operators

4.6 Individuals can choose to have information from 'registered repository operators' included in their My Health Record. Broadly described as a 'Medicare history', this includes Medicare and Pharmaceutical Benefits Scheme claims[70]; organ donor status; and immunisation records. Content from these systems is updated in My Health Record daily. Repository operators are responsible for, and manage, the quality of this data.

4.7 There are instances of administrative errors, called 'intertwined records', where a single Medicare record has been used interchangeably between two or more individuals. This most often

[69] Consideration was not given to data quality in relation to secondary use for research. The framework to guide the secondary use of My Health Record data is available online at: http://www.health.gov.au/internet/main/publishing.nsf/Content/eHealth-framework [accessed 19 November 2019].

[70] Repatriation Pharmaceutical Benefits Scheme for Department of Veterans' Affairs clients.

occurs where the individuals have similar names and dates of birth and a Medicare claim has been directed to the wrong individual's record, or of fraudulent Medicare claim data flowing onto a person's My Health Record. These errors may be notifiable data breaches, but it should be noted that no individually identifiable information is contained in Medicare *claims* data.[71] It should also be noted that intertwined record errors are not caused by the My Health Record system.

4.8 Intertwined records may be identified and corrected by the repository operator (Services Australia), or may be identified by the healthcare recipient and corrected in response to their complaint or query. Procedures are in place for both circumstances.

4.9 Services Australia stated to the ANAO that most of these issues are identified through its regular data integrity activities, which includes identifying intertwined records and investigating fraudulent claiming. In response to a 2014 Auditor–General's report, and again in 2017 in preparation for the My Health Record expansion program, Services Australia conducted additional data mining activities to identify potential intertwined and duplicate Medicare records.[72]

4.10 ADHA stated that, although there is a risk that confidence in My Health Record could be compromised when consumers identify administrative errors, the 'spotlight' effect of consumers seeing their own information may assist in driving improved overall health data quality.

Data quality: healthcare providers

4.11 Most information that is directly entered into the My Health Record system by healthcare providers is by way of structured data entry using drop down fields containing standardised clinical and medicines terminology. This promotes consistency in key records such as shared health summaries. These may be accessed and completed by providers in My Health Record via their own desktop clinical information systems which integrate with the My Health Record system.[73] ADHA works with the vendors of those systems to promote the use of the standardised terminology.

4.12 Various education and training activities for providers also sought to promote data quality:

- ADHA provided online training for providers in relation to data quality, and funded PHNs to deliver provider education activities;
- ADHA stated that My Health Record was included in Continuing Professional Development units delivered by the Royal Australian College of General Practice (for general practitioners) and the Pharmacy Guild of Australia (for pharmacists); and
- guidance to providers on improving health record data quality was developed by Royal Australian College of General Practice and the Pharmaceutical Society of Australia.

4.13 These activities have focussed primarily on general practice, pharmacies and hospitals. New data quality challenges may emerge as the focus turns to increasing the number of specialists, allied health and aged care providers using the system, as many individuals in these groups may not have accessed the awareness and education activities. As the quality of data entered into the system is

[71] Identifiable information is not visible in the Medicare claims data, which is the source of most intertwined records, but it is possible in some circumstances for Medicare *enrolment* data – which includes identifiable information – to be intertwined. ADHA stated that this has not actually occurred to date and that there are processes to respond to such a data breach, should it occur.

[72] Auditor–General Report No.27 2013–14, *Integrity of Medicare Customer Data.*

[73] Providers without conformant software can obtain read only access through a web portal.

critical to the realisation of potential My Health Record system benefits, work to monitor and improve data quality will need to continue as overall use of the system increases.

Other activities

4.14 ADHA was also involved in three other activities that sought to improve health data quality in general and, by extension, data quality in the My Health Record system:

- facilitation of national standardised e-record clinical and medicines terminology and taxonomy, specifically the Systematized Nomenclature of Medicine Clinical Terms (SNOMED-CT) that includes descriptions of diseases, clinical findings, treatments and outcomes, and the Australian Medicines Terminology that describes commonly used medicines and supports electronic medication management — these are integrated into key My Health Record documents, as explained at paragraph 4.11;
- participation in a Joint Data Quality Working Group with the Australian Commission on Safety and Quality in Health Care (ACQSHC), Australian Institute of Health and Welfare and jurisdictions, reporting to health ministers and seeking to address existing data quality problems that are coming to light through My Health Record; and
- the ACQSHC undertook ten clinical safety reviews of My Health Record, including data quality issues — the recommendations of which were addressed in improvements to the system, or incorporated into broader National Digital Health Strategy work.[74]

4.15 Another potential source of information on data quality is feedback from system users. ADHA previously measured provider awareness, adoption and attitudes towards My Health Record, but at the time of the audit was no longer doing so.

Are there appropriate arrangements to measure, evaluate and report on benefits realisation?

Arrangements to measure, evaluate and report on benefits realised from My Health Record are largely appropriate. A 2017 benefits realisation plan estimated benefits over a ten year period, and identified potential data collection and research activities to measure the intermediate outputs and longer-term (‘end’) benefits. ADHA is measuring intermediate outputs – which relate to participation and use of the system – and has commissioned some research activities to measure some longer-term benefits. These research activities are not yet organised within a plan setting out clear milestones, timeframes and sequencing of evaluation and reporting activities over the forward years.

4.16 Non-mandatory guidance on program monitoring, review and evaluation is available to entities through the Department of the Prime Minister and Cabinet (PM&C) policy implementation guidance.[75] Key elements include:

- defining success and identifying evidence needed to demonstrate outcomes;

[74] The clinical safety reviews are available from: https://www.safetyandquality.gov.au/publications/ninth-clinical-safety-review-of-the-my-health-record-system/ [accessed 15 May 2019].

[75] Department of the Prime Minister and Cabinet, *Policy implementation.* PM&C [Internet], available from: https://pmc.gov.au/government/policy-implementation [accessed 20 June 2019].

- monitoring progress towards outcomes through relevant data collection;
- regular review to assess progress and evaluation of outcomes; and
- transparent reporting of results.

4.17 ADHA developed a benefits realisation plan in 2017 which defined success for the opt-out model of the My Health Record system. This plan's purpose was to set out a strategy for managing benefits of the My Health Record system, and to make sure that benefits realisation was 'planned and budgeted, underpinned by a whole of lifecycle process … appropriately resourced [and] backed by focused governance structures'.

4.18 The plan estimated the potential health sector economic benefits from implementing My Health Record as an opt-out model. Estimates were derived from academic studies rather than being extrapolated from actual My Health Record usage, due to a lack of sufficient historical data. Estimates were reviewed by a clinical reference group and clinicians from ADHA and Health. The plan stated that 'estimates were calculated conservatively'.

4.19 Potential health sector economic benefits were estimated from 2007 to 2027[76], totalling $14.59 billion. The benefit categories identified were:

- 'Improved health outcomes: if clinicians have greater access to medication information, it will result in avoided hospital admissions and saved lives' — requiring evidence of reduced hospital admissions, lengths of stay, emergency presentations, and general practice visits;
- 'A much more efficient health system' — requiring evidence of reduced healthcare provider time gathering information and communicating with other providers;
- 'Avoided duplication of diagnostic tests' — requiring evidence of reduced expenditure on duplicate tests due to better access to pathology and diagnostic imaging information;
- 'Putting the person at the centre of their healthcare' — requiring evidence of improved patient self-management through increased use of care plans, mobile apps and advance care plans linked to My Health Record; and
- 'Enabling innovation and developments in healthcare' — requiring evidence of system improvements arising from secondary use of data and innovation in care delivery.

4.20 The plan stated that intermediate output measures would be tracked using My Health Record system data analytics. Intermediate output measures include: number of individuals and healthcare providers registered; and number and type of documents uploaded and viewed ('shared') by different types of healthcare providers. These are described in Appendix 4.

4.21 The plan also stated that additional bespoke research and statistical analyses would be necessary to measure the longer-term ('end') benefits, recognising that health system 'confounding factors' would complicate direct benefits attribution.[77] Potential research included:

- for improved health outcomes — a potential study assessing any change in adverse drug events in hospital admissions, emergency department visits and general practice visits;

[76] Not adjusted for the extended opt-out period.

[77] Such as other health policy changes over time and challenges with existing data systems.

- for a much more efficient health system — potential time in motion study of clinician time taken to gather patient information and communicate with other health professionals;
- for avoided duplication of tests — statistical analyses of pathology and diagnostic imaging Medicare data to identify reduction in growth below historical averages; and
- for putting the person at the centre of their care — potential study identifying change in service use by consumers who use My Health Record compared to those who do not.

4.22 The plan is being revised for the business case to government for future funding.

Monitoring

4.23 ADHA is monitoring the intermediate output measures described in the benefits realisation plan (see paragraph 4.20 above, and Appendix 4 for more detail on these measures). Regarding the measurement of longer-term ('end') benefits, ADHA has commissioned nine research studies, of which five have been completed (refer to Appendix 5 for a description of these). Each benefit category except for 'enabling innovation and developments on healthcare', which is dependent on making data available for secondary use research, have at least one commissioned research study relating to it. ADHA stated to the ANAO that it intended to commission a series of research projects to provide evaluative evidence across the benefit categories over time. At the time of the audit, there was no documented forward plan for delivery of this intended program of work.

4.24 In addition to the nine commissioned studies, ADHA has funded 15 'test beds' to run over two years from June 2019 to assess 'digitally-enabled models' of care delivery.[78] These projects are part of the National Digital Health Strategy and each involves use of My Health Record. Projects include testing new approaches to caring for patients with chronic conditions, those requiring post-hospital support, and those receiving palliative care. Example approaches include digital sharing of information across care settings, and use of patient mobile applications linked to My Health Record.

Review and evaluation

4.25 The projected benefits realisation period for My Health Record is ten years (to 2027, not adjusted for the extended opt-out period). As noted by the gateway review in May 2019:

> The [My Health Record] system is in place, but benefits will take time and continued effort to be fully realised. The long lead time increases risk.

4.26 PM&C's guidance states that 'evaluation plans should determine the purpose, the timing, the mechanism to be used, and how results will be shared and applied', and that entities should:

> Be strategic about the focus of the evaluation: what is the most important thing to evaluate across the whole initiative and what is the best method? Identify critical checkpoints to conduct reviews and evaluations as the initiative matures through implementation.

4.27 As noted at paragraph 4.23, the benefits realisation plan sets out a range of *potential* measurement activities, several of which have been or are being undertaken. However, neither that nor any other document set out a structured plan for undertaking data collection and research activities across future years. The benefits plan does not set out the timing or sequencing of

[78] Australian Digital Health Agency, *Digital health test beds program,* ADHA [Internet], available from https://conversation.digitalhealth.gov.au/digital-health-test-beds-program [accessed 15 August 2019]

activities. It does not identify critical checkpoints to conduct reviews and evaluations as the initiative matures, nor address the effectiveness of program administration elements.

4.28 Given that the projected benefits realisation period for My Health Record is ten years, the ADHA should develop a forward looking evaluation plan to guide the sequencing, timing and scope of activities across the coming years. This would provide a clear line of sight as to what actions will be taken and when to collect and assess relevant information. Without a plan, there is a risk that there will not be enough evidence to evaluate the longer-term effectiveness of My Health Record.

Recommendation no.5

4.29 ADHA develop and implement a program evaluation plan for My Health Record, including forward timeframes and sequencing of measurement and evaluation activities across the coming years, and report on the outcomes of benefits evaluation.

Australian Digital Health Agency response: *Agreed.*

4.30 *The Agency will develop a longer term evaluation plan, and work with the Department of Health on assumptions and modelling for benefits realisation.*

Reporting and transparency

4.31 Accountability and transparency is primarily achieved through the reporting requirements of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act). In accordance with these requirements, ADHA reports on My Health Record implementation in its corporate plan (key milestones for My Health Record)[79], annual performance statements (summary system usage statistics of healthcare recipient and provider uptake) and annual reports (achievement against entity objectives and KPIs for the My Health Record system).

Grant Hehir

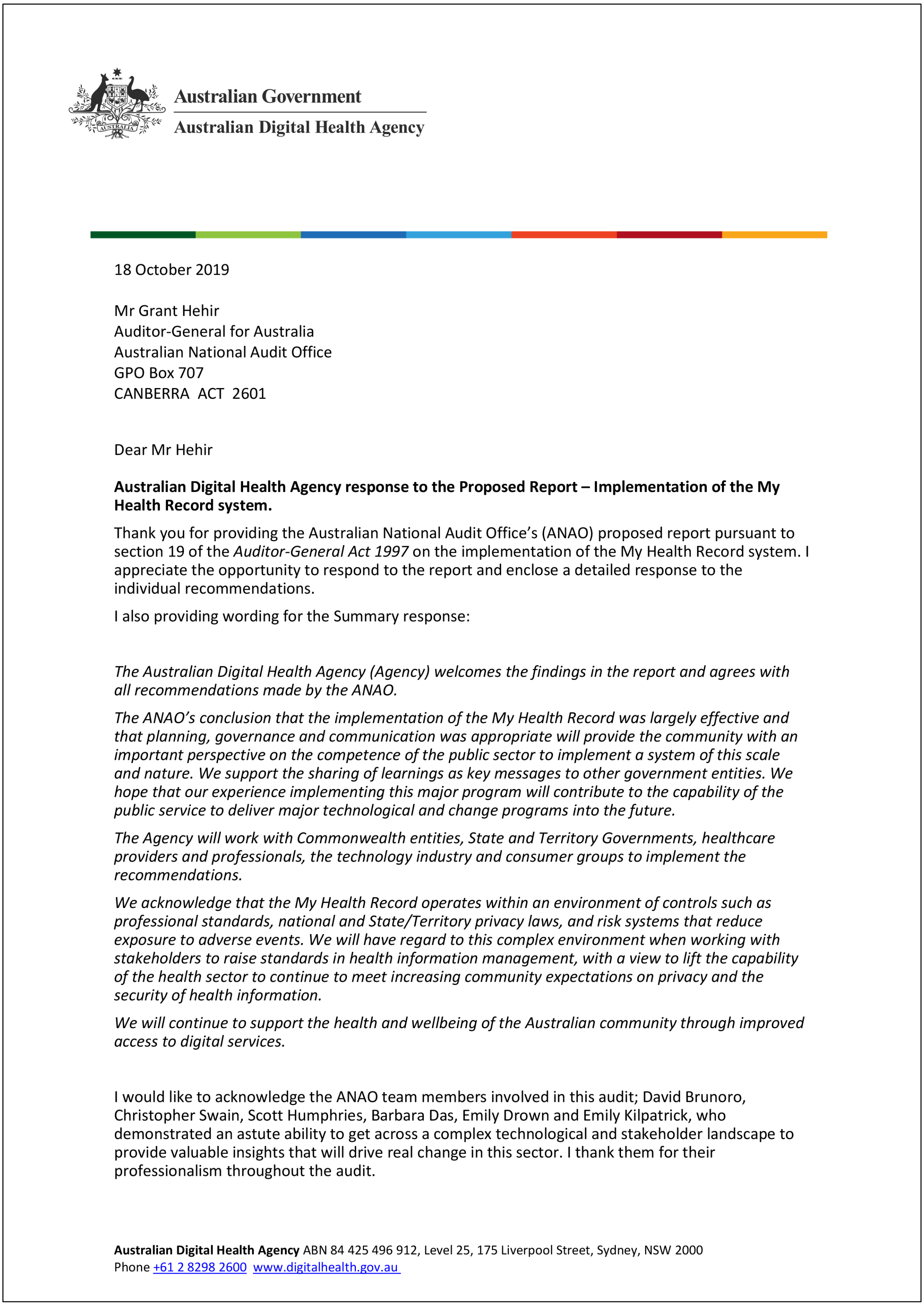
Grant Hehir
Auditor-General

Canberra ACT
25 November 2019

[79] The key milestones for My Health Record in the corporate plan include registrations and document uploads (which are a subset of, and consistent with, the intermediate output measures described at paragraph 4.23), and progress with opt-out readiness and communications activities (which are consistent with those detailed in the implementation plan described at paragraph 2.10).

Appendices

Appendix 1 Entity responses



Australian Government
Australian Digital Health Agency

18 October 2019

Mr Grant Hehir
Auditor-General for Australia
Australian National Audit Office
GPO Box 707
CANBERRA ACT 2601

Dear Mr Hehir

Australian Digital Health Agency response to the Proposed Report – Implementation of the My Health Record system.

Thank you for providing the Australian National Audit Office's (ANAO) proposed report pursuant to section 19 of the *Auditor-General Act 1997* on the implementation of the My Health Record system. I appreciate the opportunity to respond to the report and enclose a detailed response to the individual recommendations.

I also providing wording for the Summary response:

The Australian Digital Health Agency (Agency) welcomes the findings in the report and agrees with all recommendations made by the ANAO.

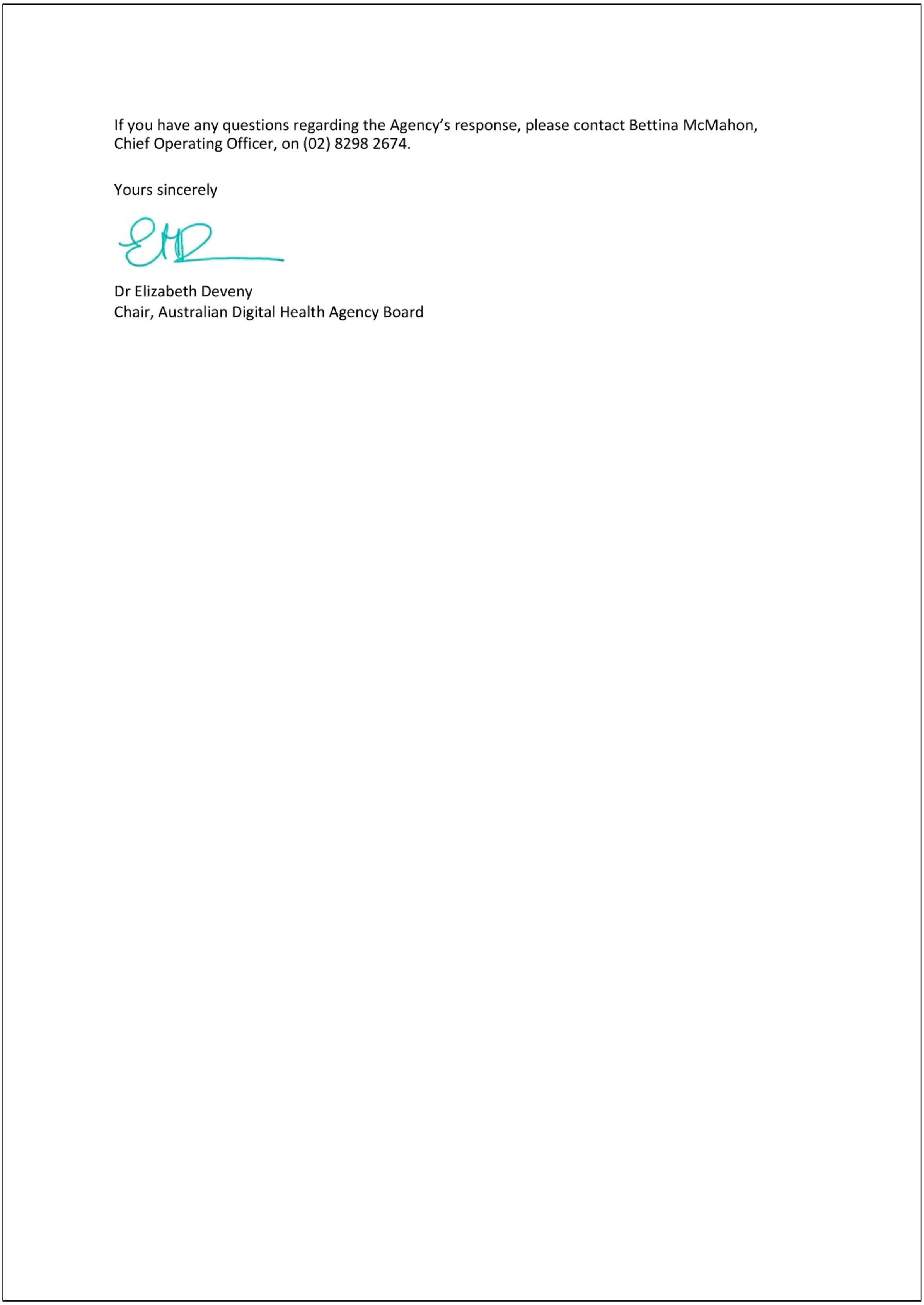
The ANAO's conclusion that the implementation of the My Health Record was largely effective and that planning, governance and communication was appropriate will provide the community with an important perspective on the competence of the public sector to implement a system of this scale and nature. We support the sharing of learnings as key messages to other government entities. We hope that our experience implementing this major program will contribute to the capability of the public service to deliver major technological and change programs into the future.

The Agency will work with Commonwealth entities, State and Territory Governments, healthcare providers and professionals, the technology industry and consumer groups to implement the recommendations.

We acknowledge that the My Health Record operates within an environment of controls such as professional standards, national and State/Territory privacy laws, and risk systems that reduce exposure to adverse events. We will have regard to this complex environment when working with stakeholders to raise standards in health information management, with a view to lift the capability of the health sector to continue to meet increasing community expectations on privacy and the security of health information.

We will continue to support the health and wellbeing of the Australian community through improved access to digital services.

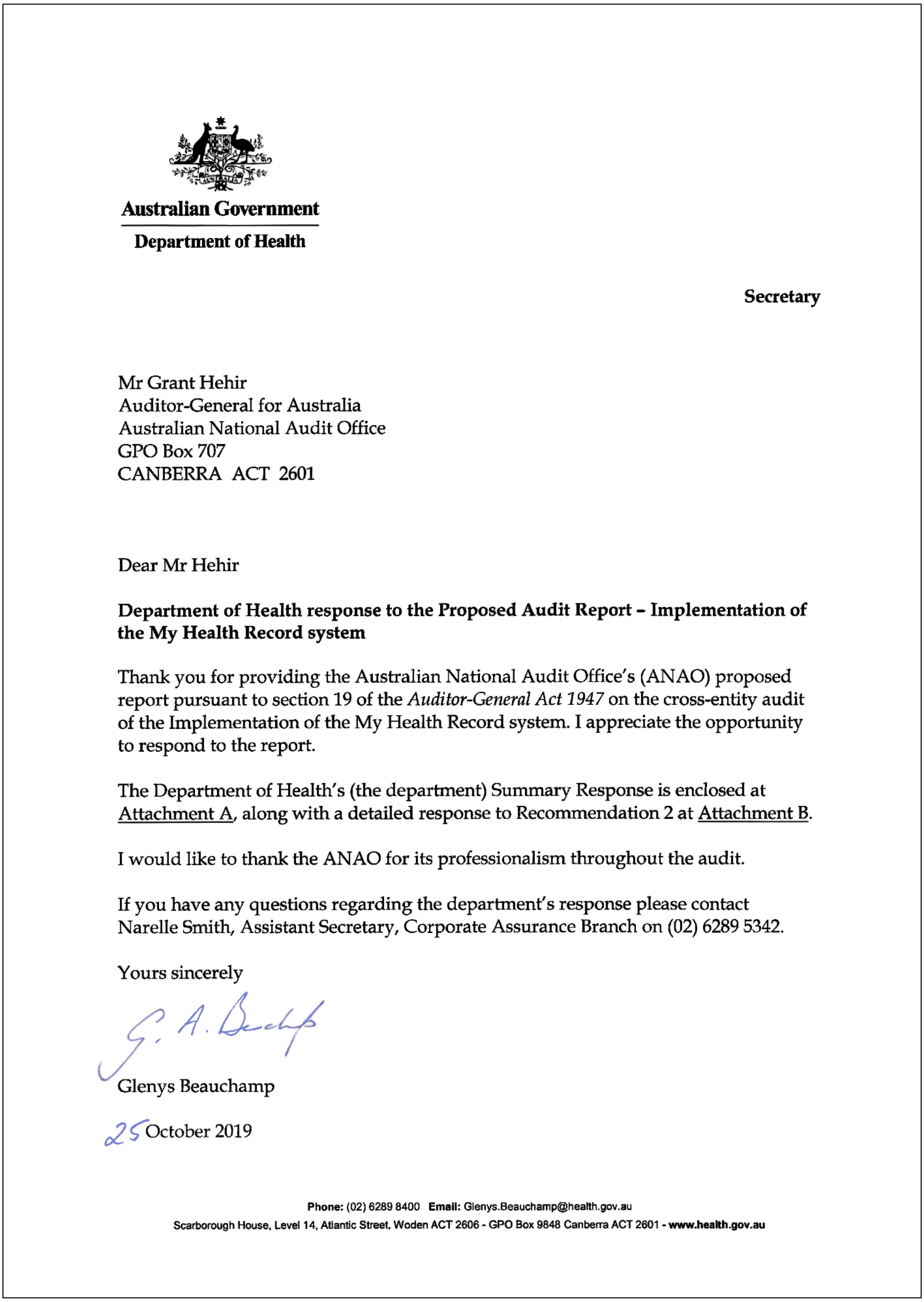
I would like to acknowledge the ANAO team members involved in this audit; David Brunoro, Christopher Swain, Scott Humphries, Barbara Das, Emily Drown and Emily Kilpatrick, who demonstrated an astute ability to get across a complex technological and stakeholder landscape to provide valuable insights that will drive real change in this sector. I thank them for their professionalism throughout the audit.



If you have any questions regarding the Agency's response, please contact Bettina McMahon, Chief Operating Officer, on (02) 8298 2674.

Yours sincerely

Dr Elizabeth Deveny
Chair, Australian Digital Health Agency Board



Australian Government

Department of Health

Secretary

Mr Grant Hehir
Auditor-General for Australia
Australian National Audit Office
GPO Box 707
CANBERRA ACT 2601

Dear Mr Hehir

Department of Health response to the Proposed Audit Report – Implementation of the My Health Record system

Thank you for providing the Australian National Audit Office's (ANAO) proposed report pursuant to section 19 of the *Auditor-General Act 1947* on the cross-entity audit of the Implementation of the My Health Record system. I appreciate the opportunity to respond to the report.

The Department of Health's (the department) Summary Response is enclosed at Attachment A, along with a detailed response to Recommendation 2 at Attachment B.

I would like to thank the ANAO for its professionalism throughout the audit.

If you have any questions regarding the department's response please contact Narelle Smith, Assistant Secretary, Corporate Assurance Branch on (02) 6289 5342.

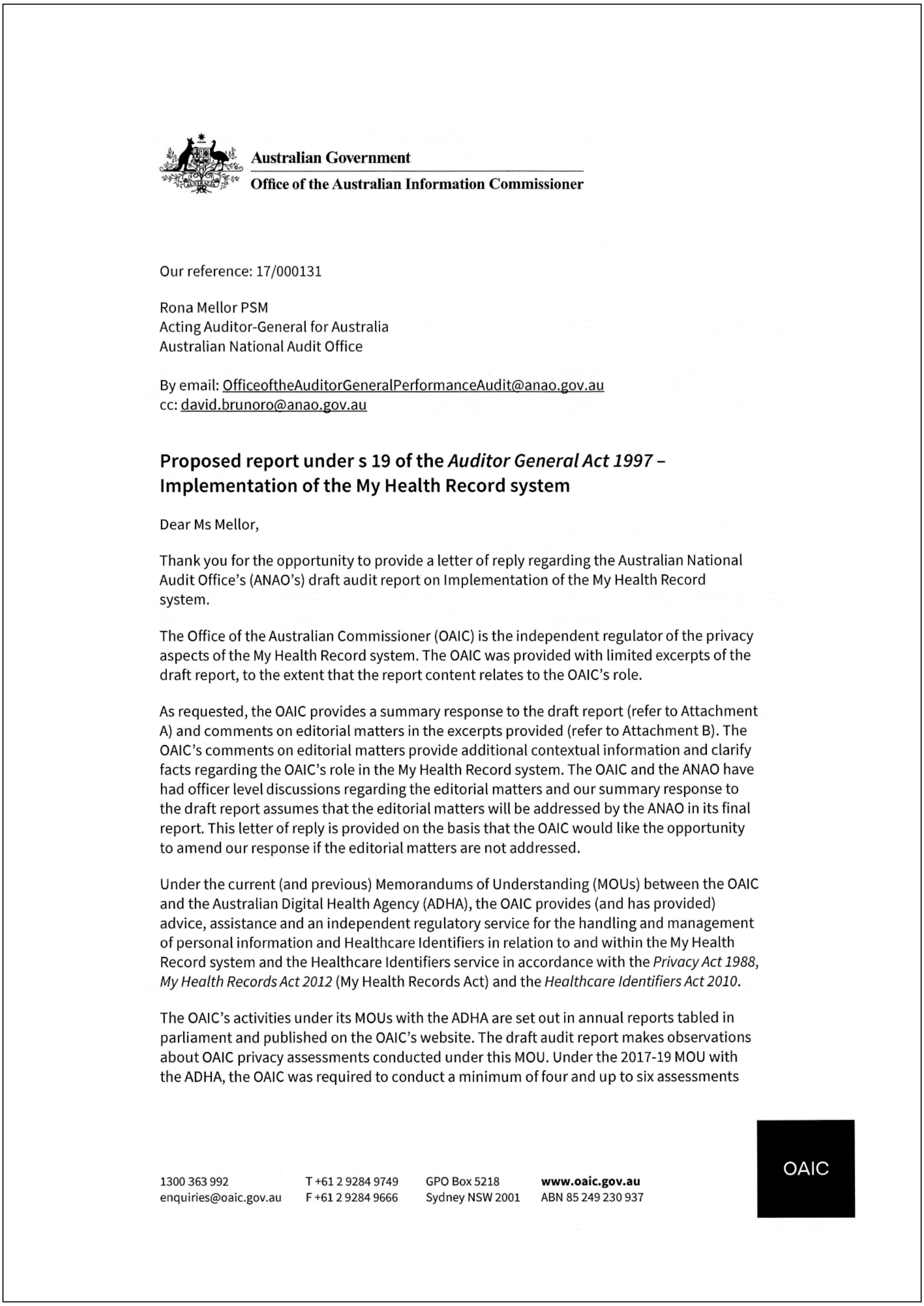
Yours sincerely

G. A. B

Glenys Beauchamp

25 October 2019

Phone: (02) 6289 8400 **Email:** Glenys.Beauchamp@health.gov.au
Scarborough House, Level 14, Atlantic Street, Woden ACT 2606 - GPO Box 9848 Canberra ACT 2601 - **www.health.gov.au**



Australian Government
Office of the Australian Information Commissioner

Our reference: 17/000131

Rona Mellor PSM
Acting Auditor-General for Australia
Australian National Audit Office

By email: OfficeoftheAuditorGeneralPerformanceAudit@anao.gov.au
cc: david.brunoro@anao.gov.au

Proposed report under s 19 of the *Auditor General Act 1997* – Implementation of the My Health Record system

Dear Ms Mellor,

Thank you for the opportunity to provide a letter of reply regarding the Australian National Audit Office's (ANAO's) draft audit report on Implementation of the My Health Record system.

The Office of the Australian Commissioner (OAIC) is the independent regulator of the privacy aspects of the My Health Record system. The OAIC was provided with limited excerpts of the draft report, to the extent that the report content relates to the OAIC's role.

As requested, the OAIC provides a summary response to the draft report (refer to Attachment A) and comments on editorial matters in the excerpts provided (refer to Attachment B). The OAIC's comments on editorial matters provide additional contextual information and clarify facts regarding the OAIC's role in the My Health Record system. The OAIC and the ANAO have had officer level discussions regarding the editorial matters and our summary response to the draft report assumes that the editorial matters will be addressed by the ANAO in its final report. This letter of reply is provided on the basis that the OAIC would like the opportunity to amend our response if the editorial matters are not addressed.

Under the current (and previous) Memorandums of Understanding (MOUs) between the OAIC and the Australian Digital Health Agency (ADHA), the OAIC provides (and has provided) advice, assistance and an independent regulatory service for the handling and management of personal information and Healthcare Identifiers in relation to and within the My Health Record system and the Healthcare Identifiers service in accordance with the *Privacy Act 1988*, *My Health Records Act 2012* (My Health Records Act) and the *Healthcare Identifiers Act 2010*.

The OAIC's activities under its MOUs with the ADHA are set out in annual reports tabled in parliament and published on the OAIC's website. The draft audit report makes observations about OAIC privacy assessments conducted under this MOU. Under the 2017-19 MOU with the ADHA, the OAIC was required to conduct a minimum of four and up to six assessments

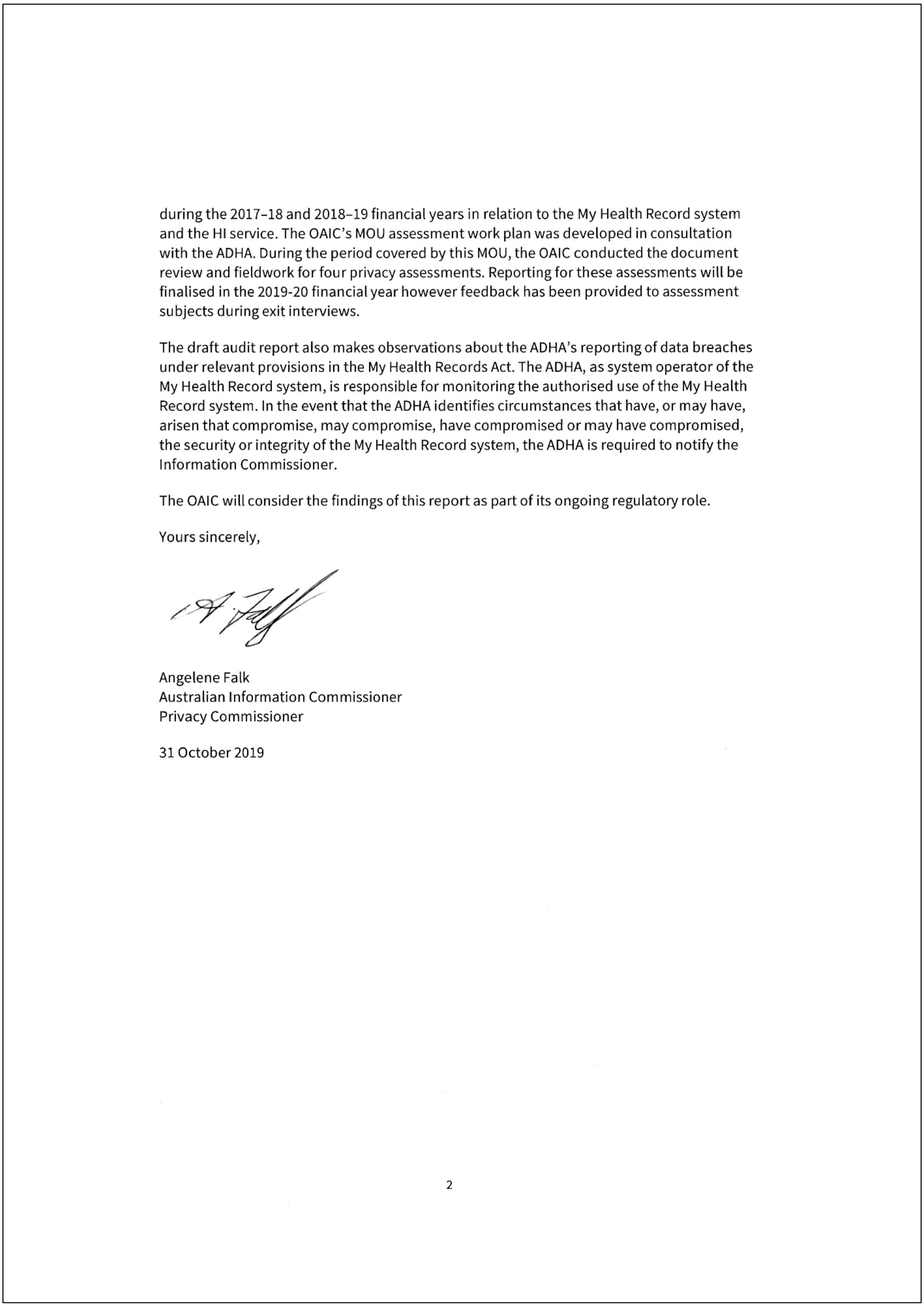
1300 363 992
enquiries@oaic.gov.au

T +61 2 9284 9749
F +61 2 9284 9666

GPO Box 5218
Sydney NSW 2001

www.oaic.gov.au
ABN 85 249 230 937

OAIC



during the 2017–18 and 2018–19 financial years in relation to the My Health Record system and the HI service. The OAIC's MOU assessment work plan was developed in consultation with the ADHA. During the period covered by this MOU, the OAIC conducted the document review and fieldwork for four privacy assessments. Reporting for these assessments will be finalised in the 2019-20 financial year however feedback has been provided to assessment subjects during exit interviews.

The draft audit report also makes observations about the ADHA's reporting of data breaches under relevant provisions in the My Health Records Act. The ADHA, as system operator of the My Health Record system, is responsible for monitoring the authorised use of the My Health Record system. In the event that the ADHA identifies circumstances that have, or may have, arisen that compromise, may compromise, have compromised or may have compromised, the security or integrity of the My Health Record system, the ADHA is required to notify the Information Commissioner.

The OAIC will consider the findings of this report as part of its ongoing regulatory role.

Yours sincerely,

Angelene Falk
Australian Information Commissioner
Privacy Commissioner

31 October 2019

Appendix 2 Privacy risk and impact assessments

1. On 12 September 2011, Health's initial Concept of Operations for the PCEHR identified privacy risks and issues related to: collection; use and disclosure; data quality; data security; openness; access and correction; use of identifiers; anonymity; cross-border data flows; and controls on sensitive information. Proposed controls included user authentication and system access controls, and regulatory compliance framework. This informed initial consultations on the development of the PCEHR.

2. On 15 November 2011, a PIA of the proposed opt-in PCEHR made 112 recommendations — 77 of which were accepted or supported in full and incorporated into the system design, 26 of which accepted in principle or in part, and 9 of which were not accepted. This assessment informed the development of the PCEHR legislation.

3. In 2014, a report on Health's public consultation on the recommendations of the 2013 PCEHR review found that 'issues of information security and misuse still exist but are not predominant concerns', and consumers valued access controls and notifications. This informed development of the opt-out model.

4. On 20 May 2015, a PIA analysed flows of personal information and potential privacy risks and impacts of an opt-out model, making 46 recommendations. The recommendations further informed the development of the opt-out model and the design of the participation trials.

5. In November 2015, a PIA assessed pathology and diagnostic imaging reports functionality and made five recommendations.

6. On 21 March 2016, a PIA assessed the design of the participation trials and concluded that privacy risks could be mitigated. Fourteen recommendations were made. This assessment informed the conduct and evaluation of the participation trials.

7. On 28 June 2016, a PIA assessed professional representative arrangements and made 14 recommendations.

8. On 18 October 2016, a PIA assessed proposals for third party mobile applications to access the My Health Record system and made 27 recommendations.

9. The evaluation report of the 2016 participation trials also identified privacy considerations for an opt-out model for people in certain situations such as those at risk of family violence and for health services staff treated in facilities where they work (these were addressed in the 2018 legislation changes).

10. On 1 December 2016, a PIA assessed the proposed bulk transfer of records to the contracted National Infrastructure Operator for record creation as part of the opt-out process and made six recommendations.

11. In July 2017, a PIA further examined privacy risks and impacts of the proposed implementation of the opt-out process and made 11 recommendations relating to opt-out communications and the process of bulk registration of records after the opt-out period.

Appendix 3 ANAO assessment of implementation status of privacy recommendations from the 2018 Senate Inquiries

Committee recommendations	Implemented
1. Record access codes:	
• Should be applied to each My Health Record by default and individuals required to choose to remove the code;	No
• The ability to override access codes in an emergency should only be available to registered healthcare providers for use in extraordinary and urgent situations.	Yes
2. Amend the *My Health Records Act 2012* to protect the privacy of children aged 14 to 17 years.	Yes
3. Amend the My Health Records Rule 2016 to extend the period for which a MHR can be suspended in the case of serious risk to the healthcare recipient.	No
4. Data which is likely to be identifiable from an individual's MHR not be made available for secondary use without the individual's explicit consent.	No
5. Strengthen the prohibition on secondary access to My Health Record data for commercial purposes.	Yes
6. Prohibit any third-party access to an individual's My Health Record without the individual’s explicit permission, except to maintain contact information.	Yes
7. Amend the *My Health Records Act 2012* and the *Healthcare Identifiers Act 2010* to ensure that it is clear that an individual's My Health Record cannot be accessed for employment or insurance purposes.	Yes
8. Access to My Health Record for government data matching be limited only to name, address, date of birth and contact information	Yes
9. Legislation be amended to make explicit that a request for record deletion is to be interpreted as a right to be unlisted, and that no cached or back-up version of a record can be accessed after a patient has requested its destruction.	Yes
10. ADHA revise its media strategy to provide more targeted comprehensive education about My Health Record.	Yes
11. ADHA identify, engage with and provide additional support to vulnerable groups to ensure that they have the means to decide whether to opt out, whether to adjust the access controls within their My Health Record and how to do this.	Yes
12. The Australian Government commit additional funding for a broad-based education campaign regarding My Health Record, with particular regard to communicating with vulnerable and hard to reach communities.	Yes
13. The Australian Government extend the opt-out period for the My Health Record system for a further twelve months.	No
14. The MHR system's operator, or operators, report regularly and comprehensively to Parliament on the management of the MHR system.	Yes

Source: ANAO analysis of ADHA and Health documentation

Appendix 4 ANAO assessment of the status of intermediate output measures for My Health Record benefits measurement

Measure	Included targets?	Data being collected?	Comments
% individuals (consumers) registered	Yes (98% by 2026-27)	Yes	% individuals registered is 90.1% at July 2018–19
% healthcare providers registered	Yes (varies by type)	Yes	Data is broken down by provider type
% providers uploading clinical information	Yes (varies by type)	Yes	Data is broken down by provider, document type
% clinical information uploaded	Yes (varies by type)	Yes	Data is broken down by document type
% system functionality implemented	Yes	Yes	Data is broken down by document type/function
% providers viewing information in MHR	Yes (varies by type)	Yes	Data is broken down by provider type
% consumers who have entered information	Yes (30% by 2026–27)	Yes	–
% consumers viewing information in MHR	Yes (52% by 2026–27)	Yes	–
% MHR data provided for secondary use	Yes (32% by 2026–27)	Not applicable	Secondary use of data commences in 2020

Source: ANAO analysis of ADHA documentation.

1. The baseline year for all categories is 2015–16.

2. Output measures for ‘healthcare providers’ are broken down by general practice, public and private hospitals, pharmacies, specialists, allied health, aged care, pathology and diagnostic imaging.

3. Output measures for ‘clinical information’ are broken down by the type of providers uploading and viewing, and by the type of document: shared health summary, discharge summary, event summary, specialist letter, MBS and PBS data, prescription records, medications views, advance care documents, care plans, age care transfer form, report patient observations/monitoring, organ donor status, child development report, pathology report, diagnostic imaging report, immunisation register, screening status and genomic information.

Appendix 5 Summary of commissioned research projects relevant to My Health Record benefits measurement

Research and evaluation reports completed at the time of the audit

1. *Evaluation of a multifaceted intervention to change clinical practice using My Health Record in primary care*, University of Wollongong, November 2018.

- Presented outcomes of an evaluation of an educational intervention, using My Health Record, for medical practitioners to encourage change in clinical behaviour and practice for pathology, diagnostic imaging ordering and de-prescribing.
- Results showed potential to effect significant changes in GPs' prescribing and pathology test-ordering behaviours.

2. *The Impact of My Health Record Use in Primary Care in Western Sydney.* Pen CS, NSW Ministry of Health, Western Sydney PHN and Western Sydney University. July 2018.

- Presented findings of a qualitative evaluation of My Health Record use among primary care practices in the Western Sydney Primary Health Network. It aimed to qualitatively examine how My Health Record may impact on clinicians and consumers by potentially improving work efficiency, reducing time spent on communication with other clinicians, improving medication safety, and reducing duplicative testing.
- Found that My Health Record can optimise patient care among particular patient groups (those who are older, and/or have complex or chronic conditions), but that while there are positive attitudes towards the system in primary care, wider implementation in more healthcare settings (e.g. specialists) was needed to increase its perceived value.

3. *The Impact of My Health Record on Primary Care*, Final Report. NPS MedicineWise and University of Melbourne. August 2018.

- Purpose was to establish a baseline of My Health Record activity for primary care practice and to develop methodologies to track the impact of My Health Record over time.
- Four studies were evaluated to establish these baselines: (1) exploring whether My Health Record activity was associated with reduced diagnostic tests for people with certain chronic diseases, and rate of prescribing of benzodiazepines; (2) determining the proportion of primary care patients with a recorded allergy or adverse drug reaction to antibiotics who had relevant information recorded in My Health Record; (3) qualitative research on the impact My Health Record has had on clinicians and consumers in improving medication safety and management; and (4) using a novel simulation approach to explore how GPs use the My Health Record in a consultation where there is potential for an adverse drug reaction.
- Found that GPs welcome the potential benefits of My Health Record, but that, at the time of the research, GPs were not yet using My Health Record as a source of trusted information in routine consultations.

4. *eHealth literacy study* – Ballarat. Deakin University. January 2019

- Presented results of an epidemiological study of eHealth Literacy in western Victoria, making recommendations to improve eHealth engagement and increase use of My Health Record by consumers.

5. *My Health Record: A South Australian General Practice Case Study*. Flinders University. November 2018.

- Researched perceptions and use of My Health Record by GPs, practice staff and patients in a single site primary care setting in South Australia, prior to and following tailored training in My Health Record.
- Found that clinician understanding of the system increased after training; perception of benefits remained stable, and use of the system was low before training with minimal change after training where clinicians held concerns about data security and privacy or the comprehensiveness of content in the system.

Research and evaluation projects still underway at the time of the audit

6. Project to develop material for Aboriginal and Torres Strait Islander health services to increase adoption and meaningful use of My Health Record. University of South Australia.

7. Project to evaluate the application of the My Health Record system in an After Hours GP service to determine the benefits of the system for that service and emergency departments. HealthDirect Australia.

8. Project to realise the potential benefits of a scalable ‘eConsultant’ telehealth model, which provides an example of the application of secure email among different healthcare providers and settings. Mater Research Institute.

9. Project to measure digital health uptake and barriers as part of an existing three-year survey of GPs and specialists. University of Melbourne.