



Executive Minute on Joint Committee of Public Accounts and Audit Report 485: Cyber Resilience

Inquiry into Auditor-General Reports 1 and 13 (2019-20)

10 June 2021 v1.0
OFFICIAL

Background

In Report 485: Cyber Resilience, the Joint Committee of Public Accounts and Audit included the following statements in the Concluding Comments of Chapter 3, relating to Auditor General Report No.13 (2019-20):

- 3.40 The Committee notes that ADHA has agreed to these recommendations and that it provided an update at the public hearing on implementation progress. ADHA has also published an Implementation Plan, with indicative timeframes.
- 3.41 The Committee appreciates that the COVID-19 pandemic has had an impact on ADHA's implementation timeframes for the audit recommendations, particularly given that a significant part of this work involves engaging with key stakeholders across the Health community. However, the Committee notes that the current Implementation Plan 'does not cover the actual changes which the Agency and others must make to implement the recommendations; this detail will be developed in 2020 through the activities described in the plan'. Accordingly, the Committee seeks an update on the key milestones and implementation dates for the audit recommendations, particularly recommendations 3 and 4 relating to cyber security.

Recommendation 6

- 3.42 The Committee recommends that the Australian Digital Health Agency (ADHA) provide an update on its 'ANAO My Health Record Performance Audit Implementation Plan' (20 February 2020), including:
- key milestones and implementation dates for each of the recommendations in Auditor-General Report No. 13 (2019-20), Implementation of the My Health Record System, with a particular focus on recommendations 3 and 4; and
 - details of the specific changes that ADHA and other stakeholders need to make to implement the recommendations.

Summary of response

Agreed.

An overview of the Agency's response to Auditor-General Report No. 13 (2019-20), Implementation of the My Health Record System is provided below:

Key milestones and implementation dates

<i>Recommendation No.1</i>	
Audit Recommendation	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 <i>(published in the audit report)</i>	Agreed. 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.
Due Date	25 November 2021
Key deliverables	<ol style="list-style-type: none"> 1) Privacy risk assessment report – completed September 2020 2) Incorporation of results into the risk management framework for the My Health Record system <ol style="list-style-type: none"> a. initial risk register updates – completed February 2021 b. shared risk management guidance – drafted May 2021 c. further updates to risk management framework, as required – ongoing
Ongoing activity	Engagement with parties involved in the shared risk landscape to manage current and emerging shared privacy risks, via existing partnership arrangements.

<i>Recommendation No.2</i>	
Audit Recommendation	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 <i>(published in the audit report)</i>	Agreed. 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.
Due Date	25 November 2021
Key deliverables	<ol style="list-style-type: none"> 1) Compliance Framework – completed February 2021 2) Emergency Access Compliance Plan – completed February 2021
Ongoing activity	Ongoing monitoring of Emergency Access; and engagement with system participants to promote a sound understanding of the legislative provision and relevant reporting arrangements, so that unauthorised use is recognised and reported to the Information Commissioner, as required.

<i>Recommendation No.3</i>	
Audit Recommendation	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 <i>(published in the audit report)</i>	Agreed. 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.
Due Date	25 November 2021
Key deliverables	1) Overview of the Agency's assurance framework for connecting systems – completed February 2021 2) Security Requirements for Connecting Systems (aligned to the Australian Government Information Security Manual) – completed February 2021
Ongoing activity	Establishment and operation of a conformance process to support the new Security Requirements for Connecting Systems.

<i>Recommendation No.4</i>	
Audit Recommendation	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 <i>(published in the audit report)</i>	Agreed. The Agency will develop, implement and regularly report on a compliance program that monitors adherence to security requirements.
Due Date	25 November 2021
Key deliverables	1) Compliance Framework – completed February 2021 2) Security and Access Compliance Plan – completed February 2021
Ongoing activity	Ongoing monitoring and reporting of adherence to security and access requirements outlined in Parts 4 & 5 of the <i>My Health Records Rule 2016</i> ; and engagement with system participants to promote a sound understanding of the legislative provision.

<i>Recommendation No.5</i>	
Audit Recommendation	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 <i>(published in the audit report)</i>	Agreed. The Agency will develop a longer term evaluation plan, and work with the Department of Health on assumptions and modelling for benefits realisation.
Due Date	25 November 2021
Key deliverables	1) My Health Record Benefits Evaluation Plan – completed January 2021
Ongoing activity	Monitoring, reporting and ongoing review of evaluation activities, as described in the My Health Record Benefits Evaluation Plan.

Changes to be undertaken by My Health Record stakeholders

In addition to the ongoing activities outlined above, there are a number of activities that My Health Record stakeholders will need to undertake, including:

- Working with the Agency on an ongoing basis to ensure shared privacy risks are identified and appropriately managed.
- Distributing guidance materials and other resources related to shared privacy risks and legislative requirements to healthcare providers, as appropriate.
- Healthcare Provider Organisations to ensure appropriate use of Emergency Access within their healthcare facilities, as outlined in section 64 of the *My Health Records Act 2012* and adherence to notification provisions outlined under section 75 of the Act.
- System Participants to implement and maintain a policy addressing security and access requirements outlined in Parts 4 & 5 of the *My Health Records Rule 2016*; and provide a copy of the relevant policy, where requested by the System Operator.
- Software developers to undertake a conformance process for the new Security Requirements for Connecting Systems, when requested by the System Operator.

Amanda Cattermole PSM

Chief Executive Officer

Australian Digital Health Agency