Australian Government
Australian Digital Health Agency

Australian Government
Department of Health

16 March 2020

Ms Lucy Wicks MP
Chair, Joint Committee of Public Accounts and Audit
Box 6021, Parliament House
CANBERRA ACT 2600
jcpaa@aph.gov.au

Dear Ms Wicks

Re: Cyber Resilience: Inquiry into Auditor-General's Reports 1 and 13 (2019-20)

The Department of Health and the Australian Digital Health Agency (Agency) provide this submission to the Joint Committee of Public Accounts and Audit to support its consideration of the *Auditor General's Report 13 (2019-20) into the Implementation of the My Health Record System* (ANAO Report).

The Agency is responsible for national digital health services and systems and leading implementation of Australia's National Digital Health Strategy on behalf of Australian governments. It is also the My Health Record System Operator. The Department has policy responsibility for improving health outcomes for Australians through digital health policies and strategies and supporting the Government's digital health agenda.

Our submission focusses on aspects of the ANAO Report, tabled on 25 November 2019, that address cyber security risks and controls.

The notion of shared risk is a theme in the Auditor General's findings which reflects the context in which the My Health Record is used and the opportunities it presents to improve healthcare in Australia. This context was recognised by the ANAO audit team and is briefly addressed in section one[1] of the ANAO Report. We provide some additional context here to support the Committee's deliberations on cyber risks impacting the My Health Record and the environment in which controls are applied.

Opportunity for technology to promote choice and reduce fragmentation

A key feature of the Australian healthcare system is the diversity of health services and the choice available to consumers. However, this diversity can create fragmentation in the way health services are provided to an individual; creating inefficiency in the system, sub-optimal experience for consumers, and affecting the quality of care and health outcomes.

Digital technology provides an opportunity to address some of these challenges in the Australian health system. The potential to have health information 'follow' a consumer through their interactions with health services – rather than remaining in silos maintained by healthcare providers – could provide a more seamless experience for a consumer and a more complete picture for healthcare providers in the course of providing care.

The Department of Health and the Agency (and its predecessor organisation) have been developing standards, infrastructure and legislation to support this vision of connected care for 15 years. The work has been guided by two National Digital Health Strategies (published in 2009 and 2018) and is supported by the COAG Health Council. Infrastructure established includes a national healthcare identifiers service, national authentication service for health, standards for digital health messages, standard national medical terminology, the My Health Record system, and legislation to govern the operation of this infrastructure.

This infrastructure provides a platform to which other IT systems connect. The Australian innovation industry provides software, data services and devices to healthcare providers and consumers in response to demand. The common thread of national infrastructure and standards has the potential to provide continuity of care in this context of diversity and choice provided by the market.

Risks arising from adoption of technology

The increasing use of technology in the health sector does not come without risk. There are three broad, interrelated areas of risks that arise from the increased data use and exchange across the health system:

- **Privacy** – the risk that an individual's personal information will be collected, used or disclosed without their knowledge, consent or as authorised by law.
- **Security** – as a control for privacy risk, if security measures fail then this increases the likelihood of a data breach occurring. Furthermore, there are risks of malicious attack designed to damage IT systems and disrupt business continuity of health services, which have occurred where security controls are not sufficient.
- **Clinical safety** – as data is increasingly integrated into the provision of care and healthcare, providers become progressively reliant on data to make clinical decisions. This means that the availability, reliability and resilience of systems is becoming ever more important.

The ANAO Report examined whether the risks relating to the My Health Record are appropriately assessed, managed and monitored within the broader context in which the system is used, and in accordance with the Commonwealth Risk Management Policy.

Current arrangements to manage shared cyber risks

The Agency currently undertakes a range of activities to manage cyber security risks across the digital health ecosystem. These include:

- **Compliance monitoring**. The Agency monitors use of the 'emergency access' function[2] and checks compliance by healthcare providers every time this is used.
- **Assurance framework for third party software**. Software that connects to the Healthcare Identifiers Service and My Health Record – both clinical systems and mobile apps for consumers – must undergo rigorous testing prior to connecting to the national infrastructure. Following connection, the Agency monitors system performance to assure that behaviour is as expected.
- **Supporting organisations whose systems connect to the My Health Record**. The Agency monitors traffic between the My Health Record and connected health systems. Should a connected system be compromised the Agency suspends access and contacts the affected organisation to provide assistance on rectification.
- **Security awareness and education**. Raising cyber security capability across the health sector through guidance, eLearning, events, newsletters, and responding to enquires.

The Office of the Information Commissioner also undertakes audits of healthcare provider compliance with their obligations under the *My Health Records Act 2012*, *Healthcare Identifiers Act 2010* and *Privacy Act 1988*. These obligations are administered in part under a Memorandum of Understanding with the Agency.

Findings by the ANAO on cyber security risks

The ANAO found that the implementation of the My Health Record has been largely effective and that risks relating to privacy and 'the core IT infrastructure' were largely well managed. The My Health Record system is secured through multi-tiered controls to mitigate cyber security risks in line with the Australian Government Information Security Manual, and the Agency monitors use of the system to identify suspicious activity and block traffic at the perimeter of the system as required.

However, the ANAO found that the degree to which 'shared risks' in cyber security were being managed was not appropriate, and recommended that the Agency work with the technology sector and healthcare providers to better assess and manage shared risks arising from use of the My Health Record system.

Alternatively expressed, the ANAO recognised the role of the My Health Record as a system that connected with other systems in line with its purpose to improve continuity for consumers across a diverse health system. It found that the Agency was appropriately managing cyber risk to the infrastructure operated by the Government, but that security controls of systems connecting to the My Health Record were not operating to the same standards.

The ANAO noted that several state and territory auditors-general have reported on health sector vulnerability to cyber attacks and that private health service providers reported a high proportion of data breaches under the *Privacy Act 1988* Notifiable Data Breaches Scheme, with almost half relating to cyber

security incidents.[3] It concluded that not all healthcare provider organisations achieve minimum cyber security levels and that this presented a broader shared cyber security risk that the Agency had a role in managing – beyond hardening the perimeter of the system.

The Agency agreed to the findings in the ANAO Report. In our response, we described how we would go about addressing the recommendations, including working with the health sector to validate the methods proposed by the ANAO to improve security and resilience of systems that connect to the My Health Record.

Response to ANAO Report and Recommendations

The Auditor-General tabled the report on 25 November 2019. The Agency has developed an Implementation Plan[4] which sets out how we intend to address the recommendations, which was approved on 20 February 2020 by the Agency Board as Accountable Authority, and is published on the Agency website.

The Implementation Plan draws on guidance from the Department of Finance[5] on understanding and managing shared risk across multiple organisations. It also incorporates quality indicators identified by the ANAO in its report tabled in August 2019 on Implementation of ANAO and Parliamentary Committee Recommendations[6].

The Agency will be engaging with industry and relevant government entities to understand the context and risks, and to agree ways in which shared risks can be effectively managed across the public and private sectors.

This engagement will consider other aspects of the health system that also control privacy and security risks, such as professional indemnity insurance, organisational accreditation requirements and professional registration standards. We will consider the need for clinical workflows to provide safe and prompt care while meeting the community's expectations for privacy, and the current level of maturity across the sector.

The Department will support the Agency in this engagement with stakeholders to provide further education and opportunities to improve conformance with agreed clinical and security standards.

The actions we take in response to the findings in the ANAO Report will be proportionate to the associated risk with careful consideration of community expectations and pressure on the health system. Our actions will also lift cyber security controls and system resilience across the health sector.

We would be happy to discuss our progress in implementing the findings with the Committee.

Yours sincerely

[redacted]

Penny Shakespeare
Deputy Secretary
Department of Health

[redacted]

Bettina McMahon
Acting Chief Executive Officer
Australian Digital Health Agency

---

[1] ANAO Report Figure 1.3 p.19 and section 1.22 p.21.
[2] This function allows a registered healthcare provider organisation to override privacy settings in circumstances involving a serious threat to an individual's life health or safety, or a serious threat to public health or public safety.
[3] ANAO Report para 3.51, p.41.
[4] https://authoring.digitalhealth.gov.au/about-the-agency/publications/anao-performance-audit-implementation-plan-publication
[5] https://www.finance.gov.au/sites/default/files/2019-11/comcover-information-sheet-understanding-and-managing-shared-risk.pdf
[6] https://www.anao.gov.au/work/performance-audit/implementation-anao-and-parliamentary-committee-recommendations-2019