


Justin Warren  


Committee Secretary  
Joint Committee of Public Accounts and Audit  
PO Box 6021  
Parliament House  
Canberra ACT 2600

19 March 2020

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

Dear Secretary,

Thank you for providing the opportunity to comment on the Cyber Resilience: Inquiry into Auditor-General's Reports 1 and 13 (2019-20). Please find my submission below.

I give my permission to publish my submission online, along with my name. Please redact my signature below and my contact email address prior to publication.

Yours sincerely,



Justin Warren

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

I thank the committee for providing the opportunity to provide a submission to the inquiry.

The issue of cyber resilience is an important one, particularly so during the trying times we now find ourselves in as a result of the COVID-19 coronavirus disease. A great many people are now using technology to maintain their connection to loved ones when they are unable to be physically present.

We depend on government entities to safeguard our information and ensure their systems are cyber resilient so that we can be assured they will remain functional and secure when we need them most.

### Implementation of the My Health Record system

It was very concerning to learn that the Australian Digital Health Agency (AHDA) had not “undertaken an end-to-end privacy risk assessment of the ongoing operation of the My Health Record system under the opt-out model.”<sup>1</sup> It is difficult for Australians to have confidence that their privacy is being protected after such a fundamental aspect of the system was changed (opt-in to out-out) if the risks associated with the system *as a whole* are not considered.

Privacy is complex, and technology systems are also complex. While it may appear that privacy is managed well in specific and narrow contexts, it is common for privacy risks to manifest due to the interaction of components. It is important to have a clear understanding of how privacy risks are managed not only in the context of the operation of the My Health Record system as a whole, but also in the broader context of My Health Record and its interaction with other systems.

For example, a privacy risk may manifest by virtue of publicly available information being correlated with information from My Health Record that would otherwise seem to pose little or no risk. A malicious actor will be unconcerned by the controls placed on key information in My Health Record if this information is readily available from another source that can then be used in conjunction with My Health Record to breach an individual's privacy. It is the outcome that is important.

The ADHA has sought to reassure the public<sup>2</sup> that their information is safe in the My Health Record system, so to learn that “ADHA did not have sufficient assurance arrangements to satisfy itself that all instances of the emergency access did not constitute an interference with privacy” we must ask how ADHA's claims can be believed.

### Lack of OAIC reviews

It is also very concerning that the Office of the Australian Information Commissioner (OAIC) completed none of the four privacy reviews it was funded to complete. This raises questions about what exactly the funding was for and how it was used. Should the money be returned? Or was the oversight of the delivery of the reviews deficient?

How can we be assured that when public monies are spent that we get what we pay for?

### Shared risks

The ADHA appears overly reliant on attestation from third parties that they have done what is required to comply with the privacy and security requirements of connecting to the My Health Record system.

- 1 Australian National Audit Office, *Implementation of the My Health Record System* (30 June 2018), <https://www.anao.gov.au/work/performance-audit/implementation-the-my-health-record-system> viewed 19 March 2020.
- 2 Australian Digital Health Agency, *Control Access to Documents* (13 February 2019) My Health Record, <https://www.myhealthrecord.gov.au/for-you-your-family/howtos/control-document-access> viewed 19 March 2020.

The health sector is consistently the single greatest source of notifiable data breaches<sup>3</sup> so it is not unreasonable to expect that access to the My Health Record system should be predicated on a demonstrated, provably robust approach to privacy and cyber resilience.

The My Health Record system is, by design, a massive, centralised repository of some of the most sensitive information about Australians that exists. Providing access to this system without high levels of assurance that those being granted access are suitably trained in cyber security, privacy, and cyber resilience is to invite disaster.

## **Trust in government agencies**

The ADHA was well aware of the concerns of the public regarding the security and privacy of their data in the My Health Record system. For the public to have faith that government is working in the public interest it is not enough to merely assert that it values our privacy, it must demonstrate that it values our privacy through its actions. To fail to conduct adequate privacy reviews suggests that agencies are more concerned with appearances than they are in doing what is necessary to safeguard our information.

## **Cyber resilience of government business enterprises and corporate commonwealth entities**

It was disappointing to learn that Australia Post was not found to be cyber resilient in the Auditor General's report<sup>4</sup> into cyber resilience of various government entities.

Entities often speak of their future plans to address identified deficiencies in managing cyber risks. While a desire to improve is laudable, it does raise questions about why these deficiencies exist in the first place. How much warning about the need to "invest sufficiently in people and ICT assets" is required before an organisation should be considered negligent for not having done more?

We are now multiple decades into the 21<sup>st</sup> century and computers are everyday items, not futuristic novelties. Is a desire to be better at some point in the future good enough? Or is the public entitled to feel that, perhaps, insufficient attention has been paid to important aspects of running things?

The committee might do well to turn its attention to the track record of entities and their previous statements regarding their intentions to do better, and how well they have delivered on those promises. At some point words must turn into deeds.

Repeated inability to live up to promises should be cause for rethinking the suitability of individuals to the task placed before them. Particularly if those individuals are extremely well compensated<sup>5</sup> for their alleged expertise compared to the average member of the public whom they serve.

3 Office of the Australian Information Commissioner, *Notifiable Data Breaches Report: July–December 2019*, <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2019/> viewed 19 March 2020.

4 Australian National Audit Office, *Cyber Resilience of Government Business Enterprises and Corporate Commonwealth Entities* (30 June 2018), <https://www.anao.gov.au/work/performance-audit/cyber-resilience-government-business-enterprises-and-corporate-commonwealth-entities> viewed 19 March 2020.

5 Australia Post, *Australia Post Annual Report* (2019) at 64, [https://auspost.com.au/content/dam/auspost\\_corp/media/documents/publications/2019-australia-post-annual-report.pdf](https://auspost.com.au/content/dam/auspost_corp/media/documents/publications/2019-australia-post-annual-report.pdf) viewed 19 March 2020.