



Australian Government

Australian Digital Health Agency

27 November 2020

Attorney-General's Department
Review of the Privacy Act 1988
PrivacyActReview@ag.gov.au

Dear Reviewer

The Australian Digital Health Agency (the Agency) has responsibility for coordinating and providing input to the ongoing development of the National Digital Health Strategy and the design, delivery and operations of the national digital healthcare system, including the My Health Record system. The Agency welcomes the opportunity to provide feedback on the review of the *Privacy Act 1988* (Privacy Act).

Key themes

The Agency's response focuses on the themes that relate to the interaction of the Privacy Act with other regulatory schemes, specifically the following questions:

65. *Have there been any challenges complying with the data breach notification requirements of other frameworks in addition to the NDB Scheme?*
66. *Should there continue to be separate privacy protections to address specific privacy risks and concerns?*
67. *Is there a need for greater harmonisation of privacy protections under Commonwealth law?*

65. Have there been any challenges complying with the data breach notification requirements of other frameworks in addition to the NDB Scheme?

One feature of the My Health Record system is its mandatory data breach reporting scheme, which was established to include actual and potential breaches. Reporting under this scheme is required even if the notifiable breach did not have any adverse impact on a person. The My Health Record scheme was established when the system commenced and was the first of its kind in national legislation.

The My Health Record data breach scheme was intended to provide transparency for consumers and the public about the safety and reliability of the My Health Record system. However, the definition of a breach under section 75 of the *My Health Records Act 2012* is very broad and substantially differs from what the community may reasonably consider to be a "breach". It also differs substantially from the notifiable data breach scheme requirements under the Privacy Act. One key difference is that mandatory reporting of data breaches under the My Health Records Act are required even where there may be no adverse impact or likely to result in harm to a consumer. This may also require notification to individuals if they are affected by the notifiable breach – even where there is no risk of harm.

In 2018 when the notifiable data breach scheme under the Privacy Act took effect the My Health Record system was made exempt. This means that entities covered by the Privacy Act and participating in the My Health Record system may be subject to two different notifiable data breach schemes.

The Agency would support some harmonisation of the My Health Record data breach requirements with those under the Privacy Act. Further consideration may need to be given whether to include potential My

Health Record data breaches in any revised scheme to maintain some of the additional protections currently provided under the My Health Records Act. It is important to recognise that state and territory public sector bodies participate in the My Health Record system but are not subject to the Privacy Act or its notifiable data breach scheme.

66. Should there continue to be separate privacy protections to address specific privacy risks and concerns?

The My Health Record system is a national public system for making health information available to consumers and their treating healthcare provider organisations when needed. The handling of personal and health information contained in a healthcare recipient's My Health Record is authorised under the Privacy Act, My Health Records Act and the *Healthcare Identifiers Act 2010* legislative frameworks.

The My Health Record legislative framework was developed through significant community consultation. The separate privacy framework provided through the My Health Records Act reflects the volume and sensitive nature of health information held in the system. It contains more stringent privacy practices and imposes greater penalties for breaches compared to the Privacy Act. It also provides healthcare recipients with greater control over their health information, including the ability to permanently delete their health information in a My Health Record at any time. The Agency acknowledges that realising the benefits of the My Health Records system requires a balance between increasing access to information and managing the inherent privacy risks of making that information more readily available. This is something the ANAO noted in its recent [performance audit of the My Health Record system](#).

At this stage it is appropriate that the privacy protections in the My Health Records Act continue alongside the broader protections set out in the Privacy Act. Nevertheless, the Agency considers that some changes to the My Health Records Act should be canvassed, including further alignment with Privacy Act concepts. For example, the Agency considers that the My Health Records Act could become less complex by adopting principles-based authorisations similar to the Australian Privacy Principles. These alignments and others are outlined in the Agency's response to the recent [independent review of the My Health Records Act](#).

Importantly, state and territory public sector bodies are significant participants in the My Health Record system but are not subject to the Privacy Act or its notifiable data breach scheme. Depending on the state or territory where these bodies operate, they may not otherwise be subject to equivalent privacy laws. The separate privacy protections contained in the My Health Records Act provide a consistent approach to privacy protections in the absence of the harmonisation of privacy laws across jurisdictions.

In addition to its role under the Privacy Act, the OAIC provides independent oversight of the privacy aspects that relate to the My Health Record system and Healthcare Identifiers Service. The OAIC has specific functions and enforcement powers over these systems, including the ability to investigate complaints about the handling of information and to receive and assess data breach notifications. In addition to this compliance and enforcement role the OAIC performs proactive education and guidance functions over these systems.

67. Is there a need for greater harmonisation of privacy protections under Commonwealth law?

Currently, there is no comprehensive privacy framework to enable a consistent approach to handling health information across different jurisdictions and public and private sectors. The current framework is made up of several pieces of legislation that regulate how health information can be collected, used, disclosed and stored at a Commonwealth and State and Territory level, applying to different participants within the healthcare ecosystem in a disparate way.

For example, the Privacy Act applies to Commonwealth government agencies and private sector health service providers (among other private sector entities) but does not apply to State or Territory authorities – except for COVID app data. Some States and Territory legislation applies to respective public sectors agencies only, while some State and Territory legislation may apply to both respective public sectors agencies and private sectors organisations that handle health information. A hospital that has both public and private elements, despite sharing administrative functions, will be subject to different legislation with different requirements. Some States do not have specific privacy legislation.

This means the same piece of health information may be subject to different privacy requirements depending on where it is collected, who collects it, where it is stored, and how it is shared. These issues are a significant hinderance to achieving interoperability in the health system a key plank of the National Digital Health Strategy so that health information can be moved easily between people, organisations and systems, costs of fragmentation can be reduced and safer, higher quality care can be delivered into the future . The issues also increase the level of difficulty for healthcare providers in understanding their obligations and create confusion for healthcare recipients as to their rights and which bodies have regulatory and oversight responsibilities.


Specific challenges include:

- Different legislative requirements across jurisdictions. For example:
 - There is no whole-of-government privacy protection in WA resulting in the information handling obligations of state agencies being unclear.
 - There are material differences in requirements for privacy collection notices between State and Commonwealth legislation.
 - There are different disclosure requirements between State and Territory legislation and Commonwealth legislation when collecting health information.
 - The ACT has unique requirements around the use and disclosure of health information compared to the Commonwealth and other jurisdictions with comparable privacy laws.
 - Different privacy protections across jurisdictions and organisations adds complexity to cross-border transfers of health information.
- Inconsistent (or non-existent) definitions within legislation for key concepts needed to support interoperability. For example:
 - There is no standard concept of “consent” that can be relied upon across jurisdictions.
 - There are differing definitions of “health information” which mean the same piece of information may be treated differently according to the jurisdiction it was collected in.

Harmonisation of privacy laws or concepts nationally would assist in overcoming the challenges in handling health information in a consistent manner, and who should regulate the matter. It would reduce confusion for consumers and organisations while supporting interoperability and associated digital innovation while maintaining strong privacy, security and clinical safeguards.

I would be happy to provide further information regarding any of these matters at your convenience.

Yours sincerely

A handwritten signature in black ink, appearing to read 'Amanda Cattermole', with a stylized flourish at the end.

Amanda Cattermole PSM
Chief Executive Officer