Australian Government
Office of the Australian Information Commissioner

Our reference: D2018/009800

Committee Chair

Senate Community Affairs Legislation Committee
By email: community.affairs.sen@aph.gov.au

Submission to the Inquiry into the My Health Records Amendment (Strengthening Privacy) Bill 2018

Dear Committee Chair,

Thank you for providing the Office of the Australian Information Commissioner (OAIC) with the opportunity to comment on the My Health Records Amendment (Strengthening Privacy) Bill 2018 (the Bill).

Under the *Privacy Act 1988* (Cth) (Privacy Act), a function of the Australian Information Commissioner and Privacy Commissioner (the Commissioner) is to examine a proposed enactment that would require or authorise acts or practices of an entity that might otherwise be interferences with the privacy of individuals, or which may otherwise have any adverse effects on the privacy of individuals.[1] The Commissioner also has the function of ensuring that any adverse effects of the proposed enactment on the privacy of individuals are minimised.[2]

The OAIC understands that the primary purpose of the Bill is to amend the *My Health Records Act 2012* (MHR Act) to strengthen the privacy framework of the My Health Record system. As outlined in the Explanatory Memorandum, among other things, the Bill will restrict the current ability of the System Operator, the Australian Digital Health Agency, to disclose health information contained in a My Health Record to law enforcement agencies and government agencies without an order by a judicial officer. The Bill will also require the System Operator to permanently delete from the National Repositories Service any health information about a healthcare recipient who has cancelled their My Health Record.

The OAIC was consulted by the Department of Health during the drafting phase of the Bill, and is supportive of these privacy enhancing measures which will provide individuals with greater certainty and control over how their My Health Record information will be handled.

[1] Privacy Act, s28(2)(a).

[2] Privacy Act, s 28(2)(c).

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

The OAIC's role

The OAIC is responsible for exercising the privacy regulatory functions of the My Health Record system. The OAIC has performed this independent regulatory role since the system commenced in 2012.

The privacy framework for the My Health Record system is currently set out in the Privacy Act, the MHR Act and the *Healthcare Identifiers Act 2010* (HI Act). The OAIC has a range of regulatory functions and enforcement powers under both the Privacy Act and MHR Act to ensure compliance with these privacy requirements.[3]

The OAIC has also entered a Memorandum of Understanding (MOU) with the Australian Digital Health Agency (the My Health Record System Operator) in relation to the OAIC's delivery of independent privacy regulatory services in relation to the My Health Record system. In addition to exercising the regulatory and enforcement functions the OAIC also performs a number of other activities under this MOU. This includes responding to enquiries and requests for advice on My Health Record privacy compliance obligations, and developing written guidance materials on privacy for users of the system. The OAIC's full range of digital health regulatory activities is set out in the MOU.

Disclosure for law enforcement purposes

Part 4, Division 2 of the MHR Act provides for the authorised collection, use and disclosure of health information included in a registered healthcare recipient's My Health Record. Under section 70 of the My Health record Act, one type of authorised use or disclosure is for law enforcement purposes.

The OAIC understands that under the current terms of section 70, a warrant would not be required to enable the System Operator to disclose My Health Record data to an enforcement body, such as the police, for law enforcement purposes. Rather, the System Operator would be authorised to use or disclose information for a law enforcement purpose, where they have a reasonable belief that the use or disclosure is reasonably necessary for that purpose. I note that these provisions are aligned with the general law enforcement exception in APP 6.2(e) of the Privacy Act.

Under proposed section 69A of the Bill,[4] the System Operator would be compelled to disclose such information only where an order has been made by a judicial officer to do so, in

---

[3] For further information about the Information Commissioner's functions in relation to the My Health Record system see *Privacy fact sheet 18: The OAIC and the My Health Record system* <https://www.oaic.gov.au/individuals/privacy-fact-sheets/health-and-digital-health/privacy-fact-sheet-18-the-oaic-and-the-my-health-record-system>. For information about the Information Commissioner's enforcement and investigative powers and regulatory approach see the My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016 <https://www.legislation.gov.au/Details/F2016L00360>.

[4] See Item 12 of the Bill.

line with the requirements in that section. This would enshrine in law the System Operator's public policy statement that it had not and would not release any information to such bodies without a court order.[5] Further, the relevant judicial officer may only make such an order where they are satisfied that, having regard to the relevant circumstances, the disclosure of the information would not, on balance, unreasonably interfere with the privacy of the affected healthcare recipient.

While the proposed legislative change would mean the MHR Act would no longer align with the exception in APP 6.2(e) of the Privacy Act, the OAIC supports the proposed amendment as a privacy enhancing measure in the context of the My Health Record system, which is a searchable network of connected registered repositories storing sensitive personal information. Further, the recent community debate around third party access to My Health Record information indicates that such a safeguard is expected by the community, and is necessary to preserve the confidentiality of the doctor-patient relationship.

Disclosure authorised by law

Section 65 of the MHR Act currently allows a participant in the My Health Record system to collect, use or disclose health information included in a healthcare recipient's My Health Record where this is required or authorised by any Commonwealth, State or Territory law. The Bill amends section 65 to instead provide that only those laws specified by new subsection 65(3) may authorise collection, use and disclosure of My Health Record information.[6] The laws prescribed by the amended section 65 would be limited and only include those which allow independent oversight bodies to handle My Health Record information in the exercise of their statutory functions, specifically the MHR Act itself, the *Auditor-General Act 1997*, the *Ombudsman Act 1976*, and laws of the Commonwealth that require or authorise the collection, use or disclosure of information for the purposes of performing the Information Commissioner's functions in relation to the My Health Record system.

The OAIC supports this amendment, which provides certainty and transparency for individuals around which laws may authorise the collection, use and disclosure of My Health Record information. The OAIC also notes that the amendment makes the necessary provision to allow the OAIC to continue exercising its privacy regulatory functions in relation to the My Health Record system.

---

[5] See the My Health Record website: < https://www.myhealthrecord.gov.au/news-and-media/my-health-record-stories/fact-sheet-police-access-my-health-record> at 10 September 2018>.

[6] See Items 8-10 of the Bill.

Retention of records

The Bill will also amend section 17 of the MHR Act to require the System Operator to permanently delete health information stored in the National Repositories Service where a person has cancelled their My Health Record.[7]

Currently, section 17 of the MHR Act requires the System Operator to retain this information until 30 years after the person's death or 130 years after the date of birth of the healthcare recipient (if the System Operator does not know the date of death of the healthcare recipient). The OAIC supports this amendment, which allows individuals to permanently delete their health information which has been collected and stored by the System Operator.

The OAIC understands that the Bill will enable the System Operator to retain some identifying and administrative information where this may be necessary for the System Operator to fulfil its functions and, among other things, to enable the System Operator to assure healthcare recipients that their cancellation request has been actioned.[8]

The OAIC also notes that the Bill specifies that the System Operator will be required to permanently destroy a healthcare recipient's record 'as soon as practicable' after the decision to cancel the healthcare recipient's registration. While the Bill does not define the meaning of 'as soon as practicable', the Explanatory Memorandum states that in practice, permanent deletion of a record will occur in 24 to 48 hours, depending on when the request is made to cancel the registration and when processes to remove data from across the system are scheduled to occur.[9]

The OAIC supports this amendment as an important measure to allow individuals to exercise control over their sensitive health information by deleting their My Health Record.

The OAIC can provide further information or assistance to the Committee as required.

Yours sincerely,

Angelene Falk
Australian Information Commissioner
Australian Privacy Commissioner

14 September 2018

---

[7] See Item 6 of the Bill.

[8] Refer to page 8 of the EM to the My Health Records Amendment (Strengthening Privacy) Bill 2018.

[9] Refer to pages 7-8 of the EM to the My Health Records Amendment (Strengthening Privacy) Bill 2018.