

25 September 2023

Australian Digital Health Agency
Connected Care Branch, Digital Solutions Division
1 Atlantic St, Phillip ACT 2606

Dear representatives at the Connected Care Branch of ADHA,

**RE: Proposed updates to the Security Requirements for the My Health Record
Connecting Systems Conformance Profile**

The Australian Privacy Foundation (APF) is the nation's pre-eminent civil society body concerned with privacy. We appreciate your invitation to contribute to proposed amendments to the Security Requirements for the My Health Record Connecting Systems Conformance Profile.

The APF maintains that data consolidation is inherently risky¹. Physically and even virtually centralised records create serious and unjustified risks. Services can be undermined by single points of failure; health care data isn't universally understandable but depends on context; consolidation produces a "honey pot" that attracts break-ins and unauthorised secondary uses and creates the additional risk of identity theft; and diseconomies of scale and scope exceed economies. We therefore strongly recommend a PIA.

¹ <https://privacy.org.au/Papers/eHealth-Policy-090828.pdf>

Proposals relating to personal health care data and health care information systems must be subject to PIA processes, including prior publication of information, consultation with affected people and their representatives and advocates, and publication of the outcomes of the study. Designs for systems and associated business processes must be based on the results of the PIA, and implementations must be rejected if they fail to embody the required features.

The recommendations we provide below concern a range of privacy considerations: (1) information security, (2) data breach prevention and notification considerations, (3) recommendations to ensure for partner health organisations and (4) recommendations for public bidding processes that may be used for software providers.

1. We welcome the development in the validation of previously breached credentials (SEC-0083). We have a concern about allowing the users to log into the portal with a previously breached credential: the Notification when the credential was previously exposed in data breaches (SEC-0580) mandates a warning to the user but indicates a prohibition to “prevent interruption to clinical workflow and not force a user to update their password during the provision of healthcare.” You request software providers to “prompt the user to update the credential before the next login”, but do not limit the number of times that the affected user might use the breached credential. In password changes, non-mandated warnings have been found to only result in approximately 1/3 of people changing their passwords, but a change of password leads to 2/3 of the changed passwords being changed to a stronger password². **We therefore recommend that this clause is supplemented with a limitation of three prompts to change the credentials previously exposed in data breaches, followed by an account lockout and recovery process.** Emergency access must be subject to post-controls³.

² <https://storage.googleapis.com/pub-tools-public-publication-data/pdf/33bc2203e7bcb5c0abe289f7432e11563fb2a238.pdf>

³ <https://privacy.org.au/Papers/eHealth-Policy-090828.pdf>

2. **We welcome the development of mandating role-based access** that allows only users authorised by the healthcare organisation as having specific My Health Record system rights may have access to that particular My Health Record functionality. **We recommend reviewing healthcare organisations' protocols to ensure the enforceability of role-based My Health record access.**

3. Speed in notifying people potentially affected by a privacy event is of the essence and needs to be emphasised in the **Mandatory Data Breach Notification (MDBM)** process. Notification delay negates most of the possible limited benefits of notification. We recommend that the ADHA considers the contractual provisions of involvement of third parties in the provision of the My Health Record Connecting Systems through any public bidding processes, specifically to ensure that **any third parties involved are legally liable to abide by the Notifiable Data Breaches scheme.**

4. ADHA is a government agency compliant with Australian Privacy Principles, which suggests that the ADHA either physically possesses a record containing the personal information that can be accessed physically or electronically or has the right or power to deal with the personal information, even if it does not physically possess or own the medium on which the personal information is stored. To avoid the fragmentation of data and sharing of data outside the control of the Australian jurisdiction, **we recommend that the My Health data and any derivations from the My Health Record, including any backups, should be stored on servers located in Australia.**

5. The revised Security Requirements include encryption as well as backup and recovery procedures. To ensure data protection in storage, **the APF also recommends to also include access logs**⁴.

Thank you for your consideration of this position.

Yours sincerely,

Dr Ausma Bernot
Member of the Board
Australian Privacy Foundation

⁴ <https://privacy.org.au/policies/info-security/>