Australian Government
Australian Digital Health Agency

Security Requirements for My Health Record Connecting Systems Conformance Profile Draft v1.1
Stakeholder feedback key themes

19 April 2024 v1.1
Approved for external use
Document ID: DH-3883:2023

The Agency released the Security Requirements for My Health Record Connecting Systems Conformance Profile (Security Profile) draft v1.1 in September 2023 and invited stakeholder feedback during a review period that extended into early November.

This document summarises the key themes from stakeholder feedback provided to the Agency.

Theme 1: Ambiguity of requirements and requirement applicability

- **What we learned**
  Stakeholders advised that it was difficult to understand precisely which requirements applied to their use case and that there was insufficient guidance to support implementation. In some cases, stakeholders sought to understand whether the requirements could be relaxed for their specific use case, citing alternative controls or mechanisms to achieve the same outcome. The most common categories of requirements referred to in this feedback included:
  - session and screen locking
  - breached credential validation
  - system patching.

- **How we are responding**
  The Agency will formally respond to all stakeholders that provided feedback relating to the applicability of specific requirements for their use case. We will endeavour to do this by the end of December 2023. The Agency will modify requirements and/or requirement wording to address the feedback where relevant and appropriate. We will also endeavour to provide additional guidance notes and other supporting material to assist software developers to understand how the requirements apply to their use case.

Theme 2: Feasibility of requirement implementation

- **What we learned**
  Stakeholders advised that certain requirements presented implementation challenges for specific software system types, particularly for desktop applications and legacy software products. In some cases, the challenges noted were related to development effort and cost in the short to medium term. The most common categories of requirements referred to in this feedback included:
  - data encryption
  - data backup and restoration

- **How we are responding**
  The Agency recognises that the effort and investment required for software systems to reach the desired level of cyber security maturity will vary, dependent on where software developers are at in their 'cyber-secure' journey. In recognition of the implementation challenges presented to us by stakeholders, we will redesign the conformance profile, to target the cybersecurity maturity uplift at 3 focus areas. The focus areas represent the highest priority cybersecurity measures that healthcare software systems must implement in the short to medium term:

  - **Authentication hardening**
    These measures collectively play a pivotal role in preventing unauthorised access and eliminating malicious actors from authenticated systems. Due to its effectiveness, multi-factor authentication is one of the *Essential Eight* from the *Strategies to Mitigate Cyber Security Incidents*. By implementing these security measures, organisations can significantly strengthen software systems against potential threats and safeguard sensitive information from unauthorised access or compromise.

  - **Security testing**
    The completion of penetration tests and application vulnerability testing by an independent third party, assists in identifying security vulnerabilities that adversaries might exploit. Thus enabling developers and security personnel to develop safeguards to protect against those identified vulnerabilities.

  - **Patching**
    Patching forms part of the Essential Eight from the Strategies to Mitigate Cyber Security Incidents. These requirements ensure the ongoing security of applications, drivers, and systems through effective patch management, responding promptly to vulnerability announcements.

  The next iteration of the conformance profile will mandate a suite of requirements from only these 3 focus areas. All other requirements will be optional and initially published as 'recommended' requirements only, with a view to being mandated in a future release.

  The Agency anticipates releasing a further draft iteration of the profile and accompanying support material, aligned to the revised approach, in Quarter 3 2024. All stakeholders will have an opportunity to review the forthcoming draft and provide any final feedback at that time.

Theme 3: Implementation timeline challenges

- **What we learned**
  Stakeholders advised that the proposed implementation phasing and timetable was unrealistic and unachievable for many software systems and the specific healthcare settings in which they operate. Some software developers have multiple software products in the market that cater to different healthcare settings, and each product may need significant changes to implement the requirements in the conformance profile. Stakeholders indicated that product roadmaps and delivery cycles would need significant modification that, in some cases, was simply not possible within the timeframes proposed.

- **How we are responding**
  The redesign of the conformance profile to prioritise implementation of requirements from the 3 high priority focus areas, has invalidated the previously proposed phasing and timetable.

  The initial reduced suite of requirements will need to be implemented by all systems within 12 months of the publication of the final version of the profile (in early 2024). The Agency will consider requests for extensions to this timeframe upon request, on a case-by-case basis. The next version of the profile that will introduce additional mandatory requirements (previously 'recommended') will be released after 12 months to reflect the evolving threat environment, with an implementation timeframe to be set in consultation with stakeholders at that time.

This iterative approach ensures a collaborative and effective implementation of enhanced security measures in healthcare software systems. The Agency appreciates the invaluable contributions and engagement of stakeholders in shaping a secure digital health landscape.

Publication date: 19 April 2024

Australian Digital Health Agency ABN 84 425 496 912, Level 25, 175 Liverpool Street, Sydney, NSW 2000 digitalhealth.gov.au
Telephone 1300 901 001 or email help@digitalhealth.gov.au

Disclaimer
The Australian Digital Health Agency ("the Agency") makes the information and other material ("Information") in this document available in good faith but without any representation or warranty as to its accuracy or completeness. The Agency cannot accept any responsibility for the consequences of any use of the Information. As the Information is of a general nature only, it is up to any person using or relying on the Information to ensure that it is accurate, complete and suitable for the circumstances of its use.

Document control
This document is maintained in electronic form and is uncontrolled in printed form. It is the responsibility of the user to verify that this copy is the latest revision.

Acknowledgements
The Australian Digital Health Agency is jointly funded by the Australian Government and all state and territory governments.