Security Requirements for My Health Record Connecting Systems Conformance Profile draft v1.1 - Responsibility Assignment Matrix

15 December 2023 v1.0
Approved for external use
Document ID: DH-3881:2023

The Agency recognises that certain conformance requirements outlined in the Security Requirements for My Health Record Connecting Systems Conformance Profile draft v1.1 (Security Profile) establish shared responsibility for implementation between software developers and healthcare provider organisations (HPO). In most cases, software developers are expected to provide the necessary software functionality, while healthcare provider organisations may play a role in ensuring that the functionality is enabled, configured, and used appropriately.

The description of responsibility for each role should serve as guidance for implementers and is based on the Security Requirements for My Health Record Connecting Systems Conformance Profile draft v1.1.

The requirements identified as establishing shared responsibility for implementation are outlined in Table 1.

Table 1. Requirement roles and responsibilities

Conformance Requirements		Roles	Responsibilities guidance
3.1 Authentication hardening			
SEC-0081	Session and screen locking	Software developer, HPO	The software developer is responsible for providing the timeout and locking functionality. The HPO has responsibility for setting the timeout period, only if the software allows it to be configured, otherwise the default setting provided by the software developer is in use.
SEC-0271	General user access	Software developer, HPO	The software developer is responsible for implementing the functionality. The HPO will determine if multi-factor authentication (MFA) is enabled based on HPO's risk profile. See SEC-0088.
SEC-0270	Privileged user access	Software developer, HPO	The software developer is responsible for implementing the functionality.

			The HPO will determine who the privileged users are, and if multi-factor authentication (MFA) is enabled based on HPO's risk profile. See SEC-0088.
SEC-0088	Disable application-level authentication	Software developer, HPO	It is acceptable for software to provide the ability to disable application-level authentication and the HPO can choose to use that option if it is provided by the software.
3.2 Access to systems and their resources			
SEC-0062	Role-based access	Software developer, HPO	The HPO will determine the roles and permissions of their users and the software will enable access to MHR functionality based on the HPO's defined roles and permissions.
SEC-0160	Access to backup files	Software developer, HPO	The HPO will determine who the "backup administrator" users are (in the software), and the software will ensure only those users can access, change, and erase backup files and data.
SEC-0070	Privileged account access	Software developer, HPO	The HPO will determine who the privileged users are (in the software), and the software will ensure only those privileged users have access to restricted functions.
SEC-0087	Disable inactive user accounts	Software developer, HPO	The software developer is responsible for implementing this functionality. The software developer may set a default period of inactivity or the HPO may choose to define a period of account inactivity that meets their needs.
3.3 Encryption			
SEC-0084	Encryption of data at rest on partition	Software developer, HPO	The HPO is responsible for ensuring all data is stored on an encrypted partition and the software will support the HPO by enforcing this and will depend on the implementation.
SEC-0125	Encryption of data at rest in database	Software developer, HPO	The HPO is responsible for ensuring all data stored in a database is encrypted and the software will support the HPO by enforcing this and will depend on the implementation.
3.8 System patching			
SEC-0300	Patch and update on desktop software	Software developer, HPO	The software developer may choose to provide an automated process to ensure that their systems are patched and updated and the HPO may be required to enable the download and installation of patches etc.
SEC-0301	Patch and update on software internally hosted	Software developer, HPO	The software developer may choose to provide an automated process to ensure that their systems are patched and updated and the HPO may be required to enable the download and installation of patches etc.
3.9 Data backup and restoration			
SEC-0151	Backup and restore functionality	Software developer, HPO	The software developer is responsible for providing the backup and restore functionality and the HPO is responsible for determining how that

			functionality is used in their implementation. The HPO determines if the software backup or enterprise-wide backup is used and will depend on the implementation.

Publication date: 15 December 2023

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

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