Australian Government
Australian Digital Health Agency

Security Requirements for My Health Record Connecting Systems Conformance Profile

19 December 2022 v1.0

Draft for external review

Document ID: DH-3583:2022

Draft version 001

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

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

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.

OFFICIAL

Document information

Key information

Owner Branch Manager – Clinical and Digital Health Standards Governance

Contact for enquiries Australian Digital Health Agency Help Centre
Phone 1300 901 001
Email help@digitalhealth.gov.au

Document version history

Version	Date	Comments	Agency reference
1.0	19/12/2022	Draft release for external review	DOC22/37985

Draft version history

dv #	Date	Author	Comments
001	19/12/2022	ADHA	Initial draft for external release and comment

Table of contents

1 Introduction

The Agency is cognisant of the inherent cyber security risks posed by systems connected to and accessing the My Health Record system, as well as potentially vulnerable aspects of the national infrastructure and all services under its care. To address this risk, a set of security requirements for systems connecting to the My Health Record system have been identified, comprising controls related to application development and web development, with controls aligned to the Australian Cyber Security Centre's (ACSC) Essential Eight Maturity Model [ACSC2021a]. These controls are selected as the areas of the ACSC Information Security Manual (ISM) [ACSC2021b] that are most relevant to the development of software for healthcare organisations.

The focus is on incorporating functionality within Clinical Information Systems (CIS) connected to the My Health Record system that will enable healthcare providers to implement better security within their organisations, while also balancing the potential impacts on software providers and on system participation.

The Agency has updated the My Health Record System Conformance Assessment Scheme (CAS) for connecting systems that refers to conformance requirements in this conformance profile.

1.1 Purpose

This document identifies mandatory and recommended security requirements for software products integrating to the My Health Record system. The content has been separated into two main sections:

1. Conformance requirements which are subject to conformance testing
2. Compliance requirements which require software vendor organisations to acknowledge and complete a declaration of compliance.

1.2 Intended audience

The intended audience includes:

- Software developers
- Department of Health and Aged Care
- Australian Commission on Safety and Quality in Healthcare
- State and territory jurisdiction representatives
- Services Australia.

1.3 Scope

This document contains both conformance and compliance security requirements that are to be applied to connecting systems that access the My Health Record system via the Business-to-Business (B2B) Gateway services.

2 Security frameworks and the My Health Record system

As described in the ISM, the ISM is a security manual "*to outline a cyber security framework that an organisation can apply, using their risk management framework, to protect their systems and data from cyber threats.*" [ACSC2021b].

The ISM is general and broad in nature and not all controls can be applied to all software. Of the controls that can be applied to software, the Agency has identified controls that provide direct benefits without imposing unreasonable imposts on the software product.

The Agency recognises that the ISM is periodically updated and the alignment to ISM controls in this profile is completed at a point in time. The version of the ISM from which the controls have been drawn is identified in the document references.

3 Use Cases

Use cases have been developed to provide a structure to the sections within this document. Vendors are to confirm which use cases are applicable to their product by reviewing the scope of each use case in Table 1.

All products are expected to conform to all the mandatory requirements (including any applicable conditional requirements) in UC.01 (common) and at least one of, or a combination of, UC.02, UC.03 or UC.04.

Use Case	Applicability
UC.01	Common requirements. This use case applies to all healthcare software systems and developer organisations.
UC.02	Healthcare software system installed on a desktop. Examples: • software installed from a CD • software downloaded from web and installed • executables and binaries.
UC.03	Healthcare software system that operates under a client – server model where the server is hosted internally within the bounds of the healthcare organisation and accessed via a thin client. Examples: • internally hosted application and data that is accessed via a web browser • on premise client/server architectures.
UC.04	Healthcare software system that operates under a client – server model where the server is hosted externally outside the bounds and control of the healthcare organisation and accessed via a thin client. Examples: • externally hosted web applications provided by 3rd party service providers • Software-as-a-Service (SaaS) • hosted cloud-services.

Table 1 – Use cases

Conformance and compliance requirements have been traced to the separate use cases to allow software vendor organisations to assess their applicability relevant to their software offering/s and organisation.

Table 2 provides an overview of this trace. Vendors are obligated to ensure their software satisfies all the mandatory requirements (including any applicable conditional requirements) for UC.01 and all the mandatory requirements (including any applicable conditional requirements) for other use cases the software product aligns with. Conditional requirements are formatted in italics in Table 2 and throughout this document.

Use Cases		Conformance Requirements		Compliance Requirements	
Number	**Description**	**Mandatory**	**Recommended**	**Mandatory**	**Recommended**
UC.01	All software offerings, all software organisations	SEC-0010, SEC-0020, SEC-0030, *SEC-0040*, SEC-0060, SEC-0061, SEC-0062, *SEC-0070*, SEC-0080, SEC-0081, SEC-0090, SEC-0100, SEC-0110, SEC-0130, SEC-0160, SEC-0250, SEC-0370	SEC-0084, SEC-0086, SEC-0087, SEC-0088, SEC-0300	*SEC-0380*, SEC-0400, SEC-0410, SEC-0420, SEC-0430, SEC-0440, SEC-0510, SEC-0520, *SEC-0550*	SEC-0530, SEC-0560
UC.02	Software installed on a desktop	SEC-0140, *SEC-0221*	SEC-0120	None	None
UC.03	Internally hosted web applications accessed via a thin client	SEC-0150, SEC-0170, SEC-0180, SEC-0190, SEC-0200, SEC-0210, *SEC-0221*, SEC-0390	SEC-0085, SEC-0120	None	None
UC.04	Externally hosted web applications accessed via a thin client	*SEC-0082*, SEC-0083, SEC-0151, SEC-0170, SEC-0180, SEC-0190, SEC-0200, SEC-0210, *SEC-0220*, SEC-0260, SEC-0270, *SEC-0271*, SEC-0390	SEC-0071, SEC-0085, SEC-0280	SEC-0131, SEC-0460, SEC-0470, SEC-0480, SEC-0490, SEC-0500, SEC-0540, *SEC-0570*, SEC-0310	SEC-0290

Table 2 – Security requirements traced to use cases

4 Conformance Requirements

This section contains mandatory and recommended software conformance requirements for connecting systems that access the My Health Record system via the Business-to-Business (B2B) Gateway services.

All products are expected to conform to UC.01 (common) and at least one of, or a combination of, UC.02, UC.03 or UC.04.

Note to reader: the unique numbering of each requirement contained within this section of the profile is not intended to be sequential. Further, any gaps in numbering are intentional and inconsequential. Requirements have been grouped according to the categories of controls outlined in the ISM or a suitable equivalent.

4.1 Mandatory requirements

This section lists the mandatory security software conformance requirements that are mandatory within the context of the related business use cases. Health software that implements a business use case must conform to the mandatory requirements for that business use case. Requirements that have a conditional priority are mandatory requirements where implementation is subject to the specified conditions being met.

4.1.1 Authentication hardening

SEC-0080	**Multi-factor authentication (MFA) options** The healthcare software SHALL support at least 2 authentication factors. These factors may include: • Passwords • One-time SMS codes • One-time password applications • Universal 2nd Factor security keys • Physical one-time password tokens • Biometrics (such as fingerprint or face identification) • Smartcards.
Priority:	Mandatory.
Applicable to:	UC.01.
Notes:	Pursuant to SEC-0088 Disable application-level authentication, healthcare organisations may choose not to enable MFA within the healthcare software. This may be due to the Healthcare organisation running authentication in the organisation's directory and authentication service such as Microsoft Active Directory. However, the clinical software shall support MFA.
Traces:	ISM Security Control 1401: Multi-factor authentication uses either: something users have and something users know, or something users have that is unlocked by something users know or are. ISM Security Control 1505: Multi-factor authentication is used to authenticate users accessing important data repositories.

SEC-0081	**Session lock and termination** For user accounts providing My Health Record functionalities (including, viewing a patient's My Health Record, editing a patient's My Health Record profile or preferences, authoring and contributing to a patient's My Health Record, and so on), the healthcare software system SHALL automatically log off an account, or require re-authentication after a configurable time period of inactivity, which can be set by the healthcare organisation.
Priority:	Mandatory.
Applicable to:	UC.01.
Notes:	Pursuant to SEC-0088 Disable application-level authentication, healthcare organisations may choose not to enable this functionality where their corporate system addresses this requirement. Healthcare organisations need to be able to define a period of inactivity after which the user's terminal may be considered unattended and vulnerable to misuse. Software as a Service providers may not be able to set a time period for each organisation, and as such may select a time period for all users.
Traces:	ISM Security Control 0853: Outside of business hours, and after an appropriate period of inactivity, user sessions are terminated, and workstations are rebooted. ISM Security Control 0428: Systems are configured with a session or screen lock that: • activates after a maximum of 15 minutes of user inactivity, or if manually activated by the user • conceals all session content on the screen • ensures that the screen does not enter a power saving state before the session or screen lock is activated • requires the user to reauthenticate to unlock the system • denies users the ability to disable the session or screen locking mechanism.

SEC-0083	**Protecting credentials** Where some components of the software system are hosted and accessible over the public internet, the system SHALL check the users' credentials with a known breached credentials service or against an external known breached password list. The healthcare software system SHALL perform this check at the time the password is set by the user and on the first login after the known breached credentials service or password list has been updated. If the password was found in a past breach the user SHALL be required to update their password before authenticating into the system.
Priority:	Mandatory.
Applicable to:	UC.04.
Notes:	A known breached credentials service is a service which provides either an application programming interface (API) to check if a password has been included in a known data breach or a list of all known passwords included in known data breaches. Refer Appendix A.1 for further implementation guidance.
Traces:	ISM Security Control 1590: Passwords/ passphrases are changed if: • they are directly compromised • they are suspected of being compromised • they appear in online data breach databases • they are discovered stored in the clear on a network • they are discovered being transferred in the clear across a network • membership of a shared account changes • they have not been changed in the past 12 months.

SEC-0270	**Multi-factor authentication (MFA) for administrators** The healthcare software system SHALL authenticate administrators into the production environment using multi-factor authentication.
Priority:	Mandatory.
Applicable to:	UC.04.
Traces:	ISM Security Control 1173: Multi-factor authentication is used to authenticate privileged users of systems.

SEC-0271 **Hosted service authentication**

If the healthcare software system is provided as a hosted service, the software SHALL require users to authenticate using multi-factor authentication.

Priority: Conditional.

Applicable to: UC.04.

Traces: ISM Security Control 1504:
Multi-factor authentication is used by an organisation's users if they authenticate to their organisation's internet-facing services.
ISM Security Control 1679:
Multi-factor authentication is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's sensitive data.

SEC-0082 **Single-factor authentication (SFA) breached credential validation**

If the healthcare software system is only using single factor authentication, then it SHALL check users' credentials with a known breached credentials service to ensure the credentials haven't been used in a previous data breach. This SHALL be done when user credentials are created and updated, and when the known breached password list has been updated.

Priority: Conditional.

Applicable to: UC.04.

Notes: A known breached credentials service is a service which provides either an API to check if a password has been included in a known data breach or a list of all known passwords included in known data breaches.
Refer Appendix A.1 for further implementation guidance.

Traces: ISM Security Control 1590:
Passwords/ passphrases are changed if:

- they are directly compromised
- they are suspected of being compromised
- they appear in online data breach databases
- they are discovered stored in the clear on a network
- they are discovered being transferred in the clear across a network
- membership of a shared account changes
- they have not been changed in the past 12 months.

4.1.2 Access to systems and their resources

SEC-0060	**User account privileges** The healthcare software system SHALL be able to run and perform all regular functionality, such as viewing the My Health Records, authoring and uploading a clinical document to the My Health Record, and so on, without the need for the user account to have administrator privileges on the operating system.
Priority:	Mandatory.
Applicable to:	UC.01.
Notes:	Users of privileged accounts are often targeted as their accounts can potentially give full access to a system. By not requiring the clinical software to run in administration mode, user accounts can be appropriately restricted without impacting the use of the clinical software.
Traces:	ISM Security Control 1508: Privileged access to systems and applications is limited to only what is required for users and services to undertake their duties.

SEC-0061	**Restricted access to the My Health Record system** The healthcare software system SHALL ONLY allow access to My Health Record system functionalities (including, viewing a patient's My Health Record, editing a patient's My Health Record profile or preferences, authoring and contributing to a patient's My Health Record, and so on) to authorised user accounts.
Priority:	Mandatory.
Applicable to:	UC.01.
Notes:	Only users designated by the healthcare organisation as having specific My Health Record system rights may have access to that particular functionality.
Traces:	ISM Security Control 0407: A secure record is maintained for the life of each system covering: • all personnel authorised to access the system, and their user identification • who provided authorisation for access • when access was granted • the level of access that was granted • when access, and the level of access, was last reviewed • when the level of access was changed, and to what extent (if applicable) • when access was withdrawn (if applicable).

SEC-0062	**Role-based access** Role-based access SHALL be used to define what functionality authorised users are able to access, for example viewing capability or viewing and authoring/uploading to the My Health Record system.
Priority:	Mandatory.
Applicable to:	UC.01.
Notes:	Role-based access enables the principle of least privilege to be adhered to, ensuring users are granted only the minimum level of permission required to do their job and perform their tasks. Limiting permissions in this way restricts the capability of a threat actor in the event of account compromise.
Traces:	ISM Security Control 0407: A secure record is maintained for the life of each system covering: • all personnel authorised to access the system, and their user identification • who provided authorisation for access • when access was granted • the level of access that was granted • when access, and the level of access, was last reviewed • when the level of access was changed, and to what extent (if applicable) • when access was withdrawn (if applicable).

SEC-0070	**Administrator functionality account privileges** If the healthcare software system provides the capability to modify system configurations, account privileges, audit logs, data files or applications then the software SHALL ensure that only privileged user accounts can perform these sensitive functions.
Priority:	Conditional.
Applicable to:	UC.01.
Traces:	ISM Security Control 1508: Privileged access to systems and applications is limited to only what is required for users and services to undertake their duties.

4.1.3 Encryption

SEC-0110	**Approved cryptographic algorithms for external communication** The healthcare software system SHALL encrypt all external communications using an Australian Signals Directorate (ASD) approved cryptographic algorithm, with the exception of metadata used for open data consumption (e.g., anonymised metadata).
Priority:	Mandatory.
Applicable to:	UC.01.
Notes:	External end points are defined as those that are accessed by people outside the bounds of the organisation, such as public API or authenticated internet-based API.
Traces:	ISM Security Control 1162: Cryptographic equipment or encryption software that implements an ASD Approved Cryptographic Protocol (AACP) is used to communicate sensitive data over public network infrastructure and through unsecured spaces.

4.1.4 Application development

SEC-0100	**Input validation** The healthcare software system SHALL check all inputs (e.g., datatypes and lengths) to ensure incorrect and inappropriate inputs are captured and managed without compromising the healthcare software system.
Priority:	Mandatory.
Applicable to:	UC.01.
Notes:	All forms of input including those from system calls should be checked to avoid injection attacks or buffer overflow attacks. The software vendor will need to identify and list all inputs and perform verification testing on each.
Traces:	ISM Security Control 0401: Platform-specific secure programming practices are used when developing software, including using the lowest privilege needed to achieve a task, checking return values of all system calls, validating all inputs and encrypting all communications.

SEC-0090	**Return values of system calls** The healthcare software system SHALL check and appropriately handle any return values for all system calls. All forms of input including those from system calls should be checked to avoid injection attacks or buffer overflow attacks.
Priority:	Mandatory.
Applicable to:	UC.01.
Notes:	This may include, but not be limited, to return values of system calls resulting from: • uploading attachments, which form part of a package sent to the My Health Record • the use of peripheral device interactions (such as barcode readers).
Traces:	ISM Security Control 0401: Platform-specific secure programming practices are used when developing software, including using the lowest privilege needed to achieve a task, checking return values of all system calls, validating all inputs and encrypting all communications.

SEC-0220	**Accredited penetration testing** If the healthcare software system has Internet accessible endpoints, portals, or API URLs that can be accessed from the Internet then those aspects of the system SHALL be penetration tested. Penetration testing SHALL be conducted periodically at an interval not exceeding 12 months since the last test, by either a suitably accredited security organisation or by suitably accredited individual testers. Identified vulnerabilities SHALL be addressed and the system re-assessed so that no residual vulnerabilities remain with a rating score higher than 6.9, as determined by the Common Vulnerability Scoring System (CVSS) v3.1.
Priority:	Conditional.
Applicable to:	UC.04.
Notes:	Refer to Common Vulnerability Scoring System Specification Document [First2019] for detailed information and documentation with respect to the Common Vulnerability Scoring System (CVSS) v3.1. Agency deems that an accredited security organisation is an organisation who is a CREST member and is penetration testing accredited, refer to https://service-selection-platform.crest-approved.org/. The Agency deems that an accredited individual is an individual who is either a: • EC-Council Certified Penetration Tester (CPENT), refer to https://www.eccouncil.org/programs/certified-penetration-testing-professional-cpent/ • EC-Council Licensed Penetration Test (LPT) Master Certified, refer to https://www.eccouncil.org/programs/licensed-penetration-tester-lpt-master/ • CREST Registered Penetration Tester (CRT), refer to https://service-selection-platform.crest-approved.org/.
Traces:	ISM Security Control 0402: Software is tested for security vulnerabilities by software developers, as well as an independent party, before it is used in a production environment.

SEC-0221	**Accredited vulnerability testing** If the healthcare software system has custom code that is installed and run locally on the client's hardware, then those aspects of the system SHALL be source code reviewed via the facilitation of a vulnerability assessment. Vulnerability assessments SHALL be conducted periodically at an interval not exceeding 12 months since the last assessment, by a suitably accredited security organisation. Identified vulnerabilities SHALL be addressed and the system re-assessed so that no residual vulnerabilities remain with a rating score higher than 6.9, as determined by the Common Vulnerability Scoring System (CVSS) v3.1.
Priority:	Conditional.
Applicable to:	UC.02, UC.03.
Notes:	Refer to Common Vulnerability Scoring System Specification Document [First2019] for detailed information and documentation with respect to the Common Vulnerability Scoring System (CVSS) v3.1. The Agency deems that an accredited security organisation is an organisation who is a CREST member and is a vulnerability assessment accredited service provider, refer to https://service-selection-platform.crest-approved.org/.
Traces:	ISM Security Control 0402: Software is tested for security vulnerabilities by software developers, as well as an independent party, before it is used in a production environment.

4.1.5 Web application development

SEC-0390	**OWASP Application Security Verification Standard** Web-based healthcare software systems SHALL follow the Open Web Application Security Project (OWASP) Application Security Verification Standard to Application Security Verification Level 2.
Priority:	Mandatory.
Applicable to:	UC.03, UC.04.
Notes:	Refer to the OWASP Application Security Verification Standard [OWASP2019].
Traces:	ISM Security Control 0971: The OWASP Application Security Verification Standard is followed when developing web applications.

SEC-0190	**HTTPS exclusively** Web-based healthcare software systems SHALL serve all web application content exclusively on HTTPS.
Priority:	Mandatory.
Applicable to:	UC.03, UC.04.
Notes:	Refer to the Guidelines for Cryptography [ACSC2021c].
Traces:	ISM Security Control 1552: All web application content is offered exclusively using HTTPS.

SEC-0210	**Client-side input validation** Web-based healthcare software systems SHALL perform client-side validation and sanitisation on all input handled by the CIS.
Priority:	Mandatory.
Applicable to:	UC.03, UC.04.
Notes:	Client-side validation can reduce the chance of cross-site script (XSS) attacks, as well as improve system performance. Examples of validation and sanitisation include: • ensuring a telephone form field contains only numerals • ensuring data used in a Structured Query Language query is sanitised properly • ensuring Unicode input is handled appropriately.
Traces:	ISM Security Control 1240: Validation and/ or sanitisation is performed on all input handled by a web application.

SEC-0200	**Input validation and sanitisation** Web-based healthcare software systems SHALL perform validation and sanitisation on a trusted service layer such as a microservice, serverless API or server-side.
Priority:	Mandatory.
Applicable to:	UC.03, UC.04.
Notes:	Refer to V1.5 Input and Output Architectural Requirements in the OWASP Application Security Verification Standard [OWASP2019].
Traces:	ISM Security Control 1240: Validation and/ or sanitisation is performed on all input handled by a web application.

SEC-0170	**Output encoding** Output encoding SHALL be performed on all outputs produced by web-based healthcare software systems.
Priority:	Mandatory.
Applicable to:	UC.03, UC.04.
Notes:	Output encoding is the process of replacing HTML control characters (e.g., <, >, ", &, etc) into their encoded representatives. This is the best mitigation against cross-site scripting attacks.
Traces:	ISM Security Control 1241: Output encoding is performed on all output produced by a web application.

SEC-0180	**HTTP security policies** Web-based healthcare software systems SHALL implement: • Content-Security-Policy • HTTP Strict Transport Security (HSTS) • X-Frame-Options response headers.
Priority:	Mandatory.
Applicable to:	UC.03, UC.04.
Traces:	ISM Security Control 1424: Web applications implement Content-Security-Policy, HSTS and X-Frame-Options response headers.

4.1.6 Application hardening

SEC-0030	**Office templates with OLE packages** Healthcare software systems SHALL NOT use or be dependent on in any way Microsoft Office Templates with Object Linking and Embedding (OLE) packages.
Priority:	Mandatory.
Applicable to:	UC.01.
Notes:	Microsoft Office OLE Packages should be managed carefully by organisations as an adversary can also create macros to perform a variety of malicious activities. By avoiding the use of OLE Packages healthcare provider organisations may place restrictions on the use of Microsoft Office OLE Packages without having an impact on functionality of the clinical software.
Traces:	ISM Security Control 1542: Microsoft Office is configured to prevent activation of Object Linking and Embedding packages.

SEC-0260	**Trusted macro execution** The healthcare software system SHALL only permit Microsoft Office Macros that are from trusted locations (refer notes) or restrict all Office Macros.
Priority:	Mandatory.
Applicable to:	UC.04.
Notes:	Refer to the ACSC Microsoft Office Macro Security [ACSC2021d].
Traces:	ISM Security Control 1487: Only privileged users responsible for validating that Microsoft Office macros are free of malicious code can write to and modify content within Trusted Locations.

SEC-0040	**Office macro signing** If the healthcare software system includes any Microsoft Office macros, the macros SHALL be digitally signed using a code signing certificate from a commercial third-party Certificate Authority.
Priority:	Conditional.
Applicable to:	UC.01.
Notes:	Microsoft Office Macros should be managed carefully by organisations as an adversary can also create macros to perform a variety of malicious activities. By signing Microsoft Office macros, healthcare provider organisations may place restrictions on the use of Microsoft Office macros while still permitting execution of macros from a third-party software provider organisation.
Traces:	ISM Security Control 1674: Only Microsoft Office macros running from within a sandboxed environment, a Trusted Location or that are digitally signed by a trusted publisher are allowed to execute.

4.1.7 System patching

SEC-0250	**Patch and updating auditing** The healthcare software system SHALL confirm that all required system components and patches are in place and current. The software shall display an error message to alert the user of any exceptions, confirming that remediation action/s are required.
Priority:	Mandatory.
Applicable to:	UC.01.
Traces:	ISM Security Control 0298: A centralised and managed approach is used to patch or update applications and drivers.

SEC-0010	**Use of Java Applets or Flash** Healthcare software systems SHALL NOT use the following technologies: • Java Applets • Flash.
Priority:	Mandatory.
Applicable to:	UC.01.
Notes:	This requirement applies specifically to '*Java Applets*' and is not relevant to Java technologies such as J2EE or J2SE. Oracle deprecated Java Applets in Java SE 9 and was removed in Java SE 11. Flash was discontinued in all major web browsers at the end of 2020, meaning that no security patches are available. Refer to https://theblog.adobe.com/adobe-flash-update/.
Traces:	ISM Security Control 1486: Web browsers do not process Java from the internet. ISM Security Control 1704: Internet-facing services, office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors are removed.

SEC-0020	**Office templates with embedded Flash, Silverlight or Shockwave controls** Healthcare software systems SHALL NOT use or be dependent on in any way Microsoft Office templates that include Flash, Silverlight or Shockwave content.
Priority:	Mandatory.
Applicable to:	UC.01.
Notes:	Microsoft has stopped support for embedded Flash, Silverlight and Shockwave content. For more details refer to Microsoft's Announcement.
Traces:	ISM Security Control 1704: Internet-facing services, office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors are removed.

4.1.8 Data backup and restoration

SEC-0130	**Minimum storage time** The healthcare software system SHALL NOT automatically delete a backup file younger than a configurable time period. The minimum time period SHALL default to 3 calendar months.
Priority:	Mandatory.
Applicable to:	UC.01.
Notes:	Provide a backup facility or integrate with a backup facility.
Traces:	ISM Security Control 1548: A data restoration process, and supporting data restoration procedures, is developed, and implemented.

SEC-0140	**User backup and restore functionality** The healthcare software system SHALL provide the user backup and restore functionality and SHALL provide the user on-screen instructions for those functions.
Priority:	Mandatory.
Applicable to:	UC.02.
Notes:	On-screen instructions should be displayed to the user, detailing how clinical data or personally identifiable data can be successfully restored from a previous successful backup.
Traces:	ISM Security Control 1548: A data restoration process, and supporting data restoration procedures, is developed and implemented.

SEC-0150	**Backup capability** The healthcare software system SHALL provide backup and restore functionality OR the vendor SHALL provide instructions on how to backup their systems in their environment using 3rd party backup/ restore software.
Priority:	Mandatory.
Applicable to:	UC.03.
Traces:	ISM Security Control 1548: A data restoration process, and supporting data restoration procedures, is developed and implemented.

SEC-0151	**Backup and restore functionality** The healthcare software system SHALL provide backup and restore functionality.
Priority:	Mandatory.
Applicable to:	UC.04.
Traces:	ISM Security Control 1511: Backups of important data, software and configuration settings are performed and retained in a coordinated and resilient manner in accordance with business continuity requirements.

SEC-0160	**Non-rewritable backups** Backup files SHALL NOT be accessible to or able to be changed or erased by general users. If stored online, the backup file SHALL only be accessible to the healthcare software system.
Priority:	Mandatory.
Applicable to:	UC.01.
Traces:	ISM Security Control 1705: Unprivileged accounts, and privileged accounts (excluding backup administrators) cannot access other account's backups.

SEC-0370	**Backup scope** The backup of data SHALL contain: • all important information • software • configuration.
Priority:	Mandatory.
Applicable to:	UC.01.
Traces:	ISM Security Control 1511: Backups of important data, software and configuration settings are performed and retained in a coordinated and resilient manner in accordance with business continuity requirements.

4.2 Recommended requirements

This section lists the recommended security software conformance requirements. Requirements listed as recommended are recommended within the context of the related business use cases. Health software that implements a business use case should conform to the recommended requirements for that business use case, even though conformance to these requirements is not mandated.

4.2.1 Authentication hardening

SEC-0088	**Disable application-level authentication** If the healthcare software system is intended to integrate with the healthcare provider organisation's Single-Sign-On (SSO) service, then the system SHOULD provide the capability for the healthcare provider organisation to disable application-level authentication.
Priority:	Recommended.
Applicable to:	UC.01.
Traces:	No applicable trace to ISM Security Controls.

SEC-0071	**Multi-factor authentication (MFA) breached credential validation** If the healthcare software system is using MFA, then it SHOULD check users' credentials with a known breached credentials service to ensure the credentials haven't been used in a previous data breach. This should be done when user credentials are created and updated, and when the known breached password list has been updated.
Priority:	Recommended.
Applicable to:	UC.04.
Notes:	A known breached credentials service is a service which provides either an API to check if a password has been included in a known data breach or a list of all known passwords included in known data breaches. Refer to Appendix A.1 for further implementation guidance.
Traces:	ISM Security Control 1590: Passwords/ passphrases are changed if: • they are directly compromised • they are suspected of being compromised • they appear in online data breach databases • they are discovered stored in the clear on a network • they are discovered being transferred in the clear across a network • membership of a shared account changes • they have not been changed in the past 12 months.

SEC-0086	**Authentication credential protection** If the healthcare software system stores passwords and other forms of passwords, such as the hash of the password, it SHOULD ensure that the passwords are stored securely. This is to be done by: • not storing passwords as plain text • ensuring that passwords are stored with a unique randomly generated salt added and encrypted using an ASD approved hashing algorithm.
Priority:	Recommended.
Applicable to:	UC.01.
Notes:	Salt needs to be unique randomly generated and a minimum of 32 bytes. It is understood and acceptable that the algorithm used to generate the salt as unique per user, may result on rare occasions in generating the same salt for different users.
Traces:	ISM Security Control 1402: Stored passwords/passphrases are protected by ensuring they are hashed, salted and stretched.

4.2.2 Access to systems and their resources

SEC-0087	**Suspension of access to systems** The healthcare software system SHOULD automatically disable an account that has been inactive for a period defined by the healthcare organisation, defaulted to a period of 45 calendar days and no longer than 3 calendar months.
Priority:	Recommended.
Applicable to:	UC.01.
Notes:	This measure is a backstop. Healthcare organisations should implement de-provisioning or account disablement where the user leaves on a permanent or temporary basis.
Traces:	ISM Security Control 1404: Access to systems, applications and data repositories is removed or suspended after one month of inactivity. ISM Security Control 1648: Privileged access to systems and applications is automatically disabled after 45 days of inactivity.

4.2.3 Encryption

SEC-0084	**Encryption of data at rest** The healthcare software system SHOULD store all data on a partition encrypted with an Australian Signals Directorate (ASD) approved cryptographic algorithms or a write only partition.
Priority:	Recommended.
Applicable to:	UC.01.
Notes:	Full disk encryption provides a greater level of protection than file-based encryption. While file-based encryption may encrypt individual files, there is the possibility that unencrypted copies of files may be left in temporary locations used by an operating system.
Traces:	ISM Security Control 0459: Encryption software used for data at rest implements full disk encryption, or partial encryption where access controls will only allow writing to the encrypted partition.

4.2.4 Application development

SEC-0120	**Approved cryptographic algorithms for internal communication** The healthcare software system SHOULD encrypt all internal communications using an Australian Signals Directorate (ASD) approved cryptographic algorithm, with the exception of metadata used for open data consumption (e.g., anonymised metadata).
Priority:	Recommended.
Applicable to:	UC.02, UC.03.
Notes:	Internal communication is defined as information that is accessed by people or systems within the bounds of the organisation. Refer to the OWASP Application Security Verification Standard [OWASP2019].
Traces:	ISM Security Control 0401: Platform-specific secure programming practices are used when developing software, including using the lowest privilege needed to achieve a task, checking return values of all system calls, validating all inputs and encrypting all communications.

4.2.5 Web application development

SEC-0085	**Digital certificate validation** The healthcare software system SHOULD validate digital certificates.
Priority:	Recommended.
Applicable to:	UC.03, UC.04.
Notes:	Certificate validation should be done by: • ensuring the certificate has not been revoked. This may be done by using a Certificate Revocation List (CRL), Online Certificate Status Protocol (OCSP) or other method • checking the certificate was valid and had not expired when the transaction took place • verifying that the certificate is from a valid Certificate Authority. Certificate pinning should be considered. Which is where, for specific web addresses a certificate is 'pinned' so that only certificates from a specific Certificate Authority are accepted. Where the network operation to access the CRL or OCSP fails, the certificate validation should not fail as a result.
Traces:	ISM Security Control 0971: The OWASP Application Security Verification Standard is followed when developing web applications.

4.2.6 System patching

SEC-0280	**Automated deployment mechanism** If the healthcare software system is provided as a hosted service the healthcare software system SHOULD have an automated mechanism to confirm and record that deployed operating system and firmware patches or updates have been installed, applied successfully and remain in place.
Priority:	Recommended.
Applicable to:	UC.04.
Traces:	ISM Security Control 0298: A centralised and managed approach is used to patch or update applications and drivers.

SEC-0300	**Patch and updating automation** The healthcare software system SHOULD provide an automated mechanism to ensure that systems, both hosted and non-hosted environments, are patched and updated and applied to client systems.
Priority:	Recommended.
Applicable to:	UC.01.
Traces:	ISM Security Control 0298: A centralised and managed approach is used to patch or update applications and drivers.

5 Compliance Requirements

This section contains mandatory and recommended software compliance requirements for connecting systems that access the My Health Record system via the Business-to-Business (B2B) Gateway services.

All products are expected to conform to UC.01 (common) and at least one of, or a combination of, UC.02, UC.03 or UC.04.

Note to reader: the unique numbering of each requirement contained within this section of the profile is not intended to be sequential. Further, any gaps in numbering are intentional and inconsequential. Requirements have been grouped according to the categories of controls outlined in the ISM or a suitable equivalent.

5.1 Mandatory requirements

This section lists the mandatory security software compliance requirements that are mandatory within the context of the related business use cases. Health software that implements a business use case must conform to the mandatory requirements for that business use case. Requirements that have a conditional priority are mandatory requirements where implementation is subject to the specified conditions being met.

5.1.1 Authentication hardening

SEC-0570	**Remote access authentication** If the software developer organisation provides support through a remote or shared desktop environment, then the healthcare software SHALL authenticate them using multi-factor authentication.
Priority:	Conditional.
Applicable to:	UC.04.
Traces:	ISM Security Control 1504: Multi-factor authentication is used by an organisation's users if they authenticate to their organisation's internet-facing services. ISM Security Control 1505: Multi-factor authentication is used to authenticate users accessing important data repositories.

5.1.2 Access to systems and their resources

SEC-0500	**Privileged access policy** The software provider organisation SHALL develop and implement a policy of ensuring privileged access to systems, applications and data repositories is validated when first requested and revalidated on an annual or more frequent basis.
Priority:	Mandatory.
Applicable to:	UC.04.
Notes:	This requirement is easiest implemented by having administrator accounts automatically expire after 12 calendar months.
Traces:	ISM Security Control 1507: Requests for privileged access to systems and applications are validated when first requested.

5.1.3 Application development

SEC-0400	**Platform-specific programming practices** Software developer organisations SHALL ensure platform-specific secure programming practices are used when developing software.
Priority:	Mandatory.
Applicable to:	UC.01.
Notes:	Refer to platform-specific guidance such as: • Common Weakness Enumeration (CWE) top 25: https://cwe.mitre.org/top25/archive/2021/2021_cwe_top25.html • Microsoft .NET secure coding guidelines: https://docs.microsoft.com/en-us/dotnet/standard/security/secure-coding-guidelines • OWASP Application Security Verification Standard [OWASP2019].
Traces:	ISM Security Control 0401: Platform-specific secure programming practices are used when developing software, including using the lowest privilege needed to achieve a task, checking return values of all system calls, validating all inputs and encrypting all communications.

SEC-0430	**Access to source code** The healthcare software system SHALL ensure that the source code cannot be accessed by unauthorised persons.
Priority:	Mandatory.
Applicable to:	UC.01.
Traces:	ISM Security Control 1422: Unauthorised access to the authoritative source for software is prevented.

SEC-0440	**Threat modelling and secure design** Software developer organisations SHALL implement threat modelling and other secure design techniques to ensure that threats to software and mitigations to those threats are identified and accounted for.
Priority:	Mandatory.
Applicable to:	UC.01.
Notes:	Refer to the Open Web Application Security Project (OWASP) Threat Modelling guide: https://owasp.org/www-community/Application_Threat_Modeling.
Traces:	ISM Security Control 1238: Threat modelling and other secure design techniques are used to ensure that threats to software and mitigations to those threats are identified and accounted for. ISM Security Control 0401: Platform-specific secure programming practices are used when developing software, including using the lowest privilege needed to achieve a task, checking return values of all system calls, validating all inputs and encrypting all communications

SEC-0520	**Separate production environment from testing and development environments** The software provider organisation SHALL operate the production environment separate from testing and development.
Priority:	Mandatory.
Applicable to:	UC.01.
Traces:	ISM Security Control 0400: Development, testing and production environments are segregated.

SEC-0540	**Modifying software in development** The software provider organisation SHALL only make modifications to the software in the development environments.
Priority:	Mandatory.
Applicable to:	UC.04.
Traces:	ISM Security Control 1419: Development and modification of software only takes place in development environments.

5.1.4 Operating system hardening

SEC-0310	**Microsoft application block rules** Environments that are running on Microsoft Windows SHALL implement Microsoft's recommended application block rules to prevent application control bypasses.
Priority:	Mandatory.
Applicable to:	UC.04.
Notes:	Microsoft recommended block rules, refer to https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules.
Traces:	ISM Security Control 1544: Microsoft's 'recommended block rules' are implemented.

5.1.5 System patching

SEC-0410	**End of support notifications** Software developer organisations SHALL notify all known customers of a software product and the Agency when it is no longer supported or no longer receiving security updates.
Priority:	Mandatory.
Applicable to:	UC.01.
Traces:	ISM Security Control 0304: Applications that are no longer supported by vendors are removed.

SEC-0420	**Security vulnerability notification** Software developer organisations SHALL notify the Australian Digital Health Agency and all customers using the software, within 14 calendar days of security vulnerabilities discovered after the software is in production/use and provide a patch or workaround to mitigate the risk posed by the security vulnerability.
Priority:	Mandatory.
Applicable to:	UC.01.
Notes:	The Australian Digital Health Agency, upon receiving a notification, shall instigate established incident management processes to assist the vendor in managing the identified vulnerability.
Traces:	ISM Security Control 0298: A centralised and managed approach is used to patch or update applications and drivers.

SEC-0460	**Patch and update drivers and firmware** The healthcare software service provider SHALL develop and enact a policy where security vulnerabilities in applications, drivers and firmware assessed as extreme risk are patched, updated or mitigated within 48 hours of the security vulnerabilities being identified by vendors, independent third parties, system managers or users.
Priority:	Mandatory.
Applicable to:	UC.04.
Traces:	ISM Security Control 1697: Patches, updates or vendor mitigations for security vulnerabilities in drivers and firmware are applied within two weeks of release, or within 48 hours if an exploit exists.

SEC-0470	**Patch and update operating system and firmware** The healthcare software service provider SHALL develop and enact a policy where security vulnerabilities in operating systems assessed as extreme risk are patched, updated or mitigated within 48 hours of the security vulnerabilities being identified by vendors, independent third parties, system managers or users.
Priority:	Mandatory.
Applicable to:	UC.04.
Traces:	ISM Security Control 1694: Patches, updates or vendor mitigations for security vulnerabilities in operating systems of internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. ISM Security Control 1697: Patches, updates or vendor mitigations for security vulnerabilities in drivers and firmware are applied within two weeks of release, or within 48 hours if an exploit exists.

SEC-0480	**Supported operating systems and ICT equipment** The software provider organisation SHALL replace or update operating systems for servers and ICT equipment when the operating systems are no longer supported (i.e., patches or updates for security vulnerabilities are no longer available).
Priority:	Mandatory.
Applicable to:	UC.04.
Traces:	ISM Security Control 1501: Operating systems that are no longer supported by vendors are replaced.

SEC-0490	**Patch and updating process** Software developer organisations SHALL implement a process to ensure systems, both hosted and non-hosted environments are patched and updated.
Priority:	Mandatory.
Applicable to:	UC.04.
Traces:	ISM Security Control 0298: A centralised and managed approach is used to patch or update applications and drivers.

5.1.6 Data backup and restoration

SEC-0131	**Backup retention** Software developer organisations SHALL ensure that all backup files are retained for a minimum of 3 months.
Priority:	Mandatory.
Applicable to:	UC.04.
Traces:	ISM Security Control 1511: Backups of important data, software and configuration settings are performed and retained in a coordinated and resilient manner in accordance with business continuity requirements.

SEC-0510	**Source code backup** Software developer organisations SHALL backup their source code regularly.
Priority:	Mandatory.
Applicable to:	UC.01.
Traces:	ISM Security Control 1511: Backups of important data, software and configuration settings are performed and retained in a coordinated and resilient manner in accordance with business continuity requirements.

SEC-0380	**Full back up testing** If the software developer organisation offers backup services, the backup SHALL be tested through a full restoration at least once when initially implemented, and then each time fundamental information technology infrastructure changes occur.
Priority:	Conditional.
Applicable to:	UC.01.
Traces:	ISM Security Control 1515: Restoration of systems, software and important data from backups is tested in a coordinated manner as part of disaster recovery exercises.

SEC-0550	**Backup frequency** If the software developer organisation offers backup services, the backup SHALL be performed at least daily.
Priority:	Conditional.
Applicable to:	UC.01.
Notes:	It is preferable to automate the backup service, where possible.
Traces:	ISM Security Control 1511: Backups of important data, software and configuration settings are performed and retained in a coordinated and resilient manner in accordance with business continuity requirements.

5.2 Recommended requirements

This section lists the recommended security software compliance requirements. Requirements listed as recommended are recommended within the context of the related business use cases. Health software that implements a business use case should conform to the recommended requirements for that business use case, even though compliance to these requirements is not mandated.

5.2.1 Application development

SEC-0560	**Independent library testing** Software developer organisations SHOULD test independent libraries used within their software for security vulnerabilities, including testing by independent testers.
Priority:	Recommended.
Applicable to:	UC.01.
Traces:	ISM Security Control 0402: Software is tested for security vulnerabilities by software developers, as well as an independent party, before it is used in a production environment.

SEC-0530	**Separate testing environment from development environments** The software provider organisation SHOULD operate development and testing as segregated environments.
Priority:	Recommended.
Applicable to:	UC.01.
Traces:	ISM Security Control 0400: Development, testing and production environments are segregated.

5.2.2 Operating system hardening

SEC-0290	**Restriction of executables** The healthcare software system's environment SHOULD restrict the execution of executables, software libraries scripts and installers to a set of known and approved items.
Priority:	Recommended.
Applicable to:	UC.04.
Traces:	ISM Security Control 1657: Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.

Appendix A Implementation advice

A.1 Breached password service

Services exist that allow for the checking of passwords and whether they have been exposed within a security breach. These services differ from just password checking as they do not just use an algorithm; they use a database of known breach information.

These services are highly effective at reducing compromises to systems that only use single factor for authentication such as username/id and password. However, they should be used in conjunction with other controls such as Multi-factor Authentication mechanisms, since breached lists are only updated when the breached lists are discovered by the Breached Password Services operators.

Several industries perform this check on their customer accounts on registration and credential change as a good control against password spray and other security attacks.

Some useful guidance links include:

- 2019-130: Password spray attacks – detection and mitigation strategies [ACSC2019]
- Creating Strong Passphrases [ACSC2021e]

One way to check your credentials is by going to '*Have I been Pwned*'.

The breach service mentioned by ACSC "*Have I Been Pwned*" (HIBP) has an API for cloud use or a method for offline use that requires manual syncing to the resource.

A risk-based approach should be used as for how often an organisation should update their breached password list if they choose the offline method of use.

API: https://haveibeenpwned.com/API/v3.

Password Lists: https://haveibeenpwned.com/Passwords.

Note: There may be other services that can be used, this is referenced here due to being mentioned by ACSC.

Acronyms

Acronym	Description
ACSC	Australian Cyber Security Centre
API	Application Programming Interface
ASD	Australian Signals Directorate
B2B	Business-to-business
CAS	Conformance Assessment Scheme
CIS	Clinical Information System
CPENT	(EC-Council's) Certified Penetration Tester
CREST	Council of Registered Ethical Security Testers
CRL	Certificate Revocation List
CRT	CREST Registered Penetration Tester
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
HSTS	HTTP Strict Transport Security
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Sockets Layer (SSL)
ICT	Information and Communications Technology
ISM	(Australian Government) Information Security Manual
J2EE	Java 2 Platform Enterprise Edition
J2SE	Java 2 Standard Edition
LPT	(EC-Council) Licensed Penetration Test
MFA	Multi-factor authentication
OCSP	Online Certificate Status Protocol
OLE	Object Linking and Embedding
OWASP	The Open Web Application Security Project
SaaS	Software as a Service
SFA	Single-factor authentication
XSS	Cross-site Scripting
UC	Use cases developed to provide a structure to the sections within this document.
URL	Uniform Resource Locator

Glossary

Term	Meaning
Clinical Information System	A system that deals with the collection, storage, retrieval, communication and optimal use of health-related data, information, and knowledge. A clinical information system may provide access to information contained in an electronic health record, but it may also provide other functions such as workflow, order entry, and results reporting.
CREST	An organisation that was initially set up as a response to unregulated penetration vulnerability testing. A lack of regulation led to a lack of uniform methodology and varying outcomes for testing subjects.
Cryptographic Algorithm	An algorithm used to perform cryptographic functions such as encryption, integrity, authentication, digital signatures or key establishment.
CVSS	An open framework for communicating the characteristics and severity of software vulnerabilities.
External end points	Accessed by people outside the bounds of the organisation, such as public API or authenticated internet-based API.
Healthcare software system	Software which provides healthcare information to either healthcare providers, healthcare consumers or both.
Internal communication	Information that is accessed by people or systems within the bounds of the organisation.
OWASP	Open Web Application Security Project which provides comprehensive resources for software developers that should be followed when developing web applications.
Penetration test	A method of evaluating the security of an ICT system by seeking to identify and exploit vulnerabilities to gain access to systems and data. Also called a 'pen test', it is a test using real-world targeted cyber intrusion scenarios in an attempt to achieve a specific goal, such as compromising critical systems or information.
Privileged user	A user who can alter or circumvent a system's security measures. This can also apply to users who could have only limited privileges, such as software developers, who can still bypass security measures. A privileged user can have the capability to modify system configurations, account privileges, audit logs, data files or applications.
Salt	A unique, randomly generated string that is added to each password as part of the hashing process. As the salt is unique for every user, an attacker has to crack hashes one at a time using the respective salt rather than calculating a hash once and comparing it against every stored hash. This makes cracking large numbers of hashes significantly harder, as the time required grows in direct proportion to the number of hashes.
SHALL	When appearing in a conformance requirement, this verb SHALL indicates a mandatory requirement. Its negative form SHALL NOT indicates a prohibition.
SHOULD	When appearing in a conformance requirement, this verb SHOULD indicates a recommendation. Its negative form SHOULD NOT indicates an option that should not be supported.

Term	Meaning
Software as a Service	Software that is either supplied as a cloud-based service or deployed over the Internet to run locally. Licences and support for SaaS systems are commonly provided on a subscription basis, but other models are also used.
Vulnerability assessment	A documentation-based review of a system's design, an in-depth hands-on assessment, or automated scanning with software tools. In each case, the goal is to identify as many security vulnerabilities as possible.

References

ACSC2019 *2019-130: Password spray attacks – detection and mitigation strategies*, Australian Cyber Security Centre, August 2019

ACSC2021a *Essential Eight Maturity Model*, Australian Cyber Security Centre, October 2021

ACSC2021b *Information Security Manual*, Australian Cyber Security Centre, September 2021

ACSC2021c *Guidelines for Cryptography*, Australian Cyber Security Centre, September 2021

ACSC2021d *Microsoft Office Macro Security*, Australian Cyber Security Centre, October 2021

ACSC2021e *Creating Strong Passphrases*, Australian Cyber Security Centre, October 2021

FIRST2019 *Common Vulnerability Scoring System Specification Document*, Forum of Incident Response & Security Teams, August 2019

https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf

OWASP2019 *Application Security Verification Standard 4.0*, Section V4.0 Access Control Verification Requirements, Open Web Application Security Project, 2019

https://github.com/OWASP/ASVS/raw/v4.0.3/4.0/OWASP%20Application%20Security%20Verification%20Standard%204.0.3-en.pdf