Australian Government
Australian Digital Health Agency

My Health Record Connecting Systems Security Conformance Profile
Guidance on Penetration and Vulnerability Testing

12 February 2025 v1.0
Approved for external use
Document ID: DH-4118:2025

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

Product or document version history

Product or document version	Date	Release comments
V1.0	12/02/2025	Supporting Document For My Health Record Connecting Systems Security Conformance Profile

1 Introduction

1.1 Purpose

This document provides assistance for software developers and software providers developing systems that connect with My Health Record in navigating the process of procuring penetration testing and vulnerability assessment services to meet the related security requirements outlined in the My Health Record Connecting Systems - Security Conformance Profile v1.0.

1.2 Intended audience

The intended audience are participants in the My Health Record system, including:

- Software developers, and registered contracted service providers (CSP) of CISs
- Health jurisdictions, health departments and registered healthcare providers that utilise CISs
- Registered repository operators

1.3 Scope

This document is limited to discussing advice on how software developers and software providers can engage a security testing organisation to perform security testing on software that meet Australian Government Information Security Management requirements.

It does not cover software that does not access the My Health Record system B2B Gateway services and does not include software using the Fast Healthcare Interoperability Resources® (FHIR®) Gateway (also previously known as the Mobile Gateway).

2 Steps to engage security testing organisation for penetration and vulnerability testing

Ensuring your software complies with the security requirements set by the My Health Record Connecting Systems Security Conformance Profile (Security Conformance Profile) is essential for protecting sensitive data and maintaining compliance.

This guide helps software developers and software providers in navigating the process of procuring penetration testing and vulnerability assessment services.

1. Understand Security Conformance Profile Requirements

Start by familiarising yourself with the profiles' guidelines, especially those related to software development and penetration testing. Focus on secure software design, coding practices, and regular security assessments.

My Health Record Connecting Systems - Security Conformance Profile v1.0 | Digital Health Developer Portal

2. Identify Your Testing Needs

Determine the specific security testing services your system requires, based on its accessibility and security posture:

- **Penetration testing**: For systems accessible from the internet, this involves simulating attacks to find potential vulnerabilities.

  or

- **Vulnerability testing**: For systems not accessible from the internet, focuses on finding and reporting potential weaknesses without active exploitation.

Clearly defining your requirements will help you communicate effectively with potential testing providers.

3. Search For CREST-Accredited Providers

Visit the CREST website to find a list of accredited providers. Look for testers with certifications such as CREST Registered Penetration Tester (CRT) or CREST Certified Tester (CCT), as this confirms the skills and expertise in penetration testing.

Please contact the Agency if the software provider intends to use a security organisation which does not hold CREST membership, prior to committing to and commencing a testing engagement and for more information on implementing this requirement.

4. Evaluate Providers

- **Check Credentials**: Ensure the providers have the relevant certifications (e.g., CREST, CRT, or CCT) and experience in your industry.
- **Review Case Studies:** Assess their previous work to understand their method and success especially in the projects within the healthcare or government sectors.
- **Get Recommendations:** Request references or recommendations from industry peers who have engaged their services.
- **Check Methodology:** Confirm that vulnerabilities will be assessed and reported using current Common Vulnerability Scoring System (CVSS), which provides a standardised method to prioritise risk based on the severity.

- The Security Profile refers specifically to “Vulnerability Scoring System (CVSS) v3.1 or v4.0” See Appendix A4 of the profile.

5. Request detailed proposals

Contact multiple providers to request detailed proposals. These should include:

- **Scope of Work:** Clearly define what you want to be tested. Be sure to include follow up evaluations when identified vulnerabilities are addressed.
- **Request Methodologies:** Understand their approach to penetration testing, including adherence to OWASP standards.
- **Request Timelines:** Know how long the testing process will take.
- **Costs:** Get a breakdown of costs to compare value for money.
- **Conformance Requirements:** Refer to the Security Conformance Profile requirements and include in the testing scope requirements relevant to your product.

6. Verify credentials

Ensure the provider's certifications are current and valid to maintain compliance and reliability. You can verify this on the CREST website.

7. Review Proposed Contracts and SLAs

Thoroughly review the contracts and service level agreements (SLAs). Pay attention to key aspects including timelines, deliverables, confidentiality clauses, liability limitations and guarantees provided by the tester.

It is advisable to define clear evaluation criteria and evaluation methodology before reviewing proposals or conducting interviews.

8. Conduct Interviews

If possible, arrange interviews with potential testers to discuss your specific needs and assess their expertise, methodologies and approach to meeting requirements.

It is advisable to define clear evaluation criteria and evaluation methodology before reviewing proposals or conducting interviews.

9. Make a Decision

Select the provider that aligns best with your project requirements, delivers a comprehensive service, and maintains a transparent and reliable approach.

10. Monitor and Review

During the testing process, maintain communication with the tester. Regularly review their findings and recommendations to ensure progress is still on track and issues are addressed promptly.

11. Remediate Identified Vulnerabilities

Promptly address any vulnerabilities found during the penetration or vulnerability test and implement the recommended security measures.

As per requirements SEC-0220 and SEC-0221 retesting should be completed if any identified vulnerabilities with a rating score higher than 6.9. Software provider organisation should provide a testing report that confirms no residual vulnerabilities have a rating score higher than 6.9.