nehta

# NESAF Release 3.1

## Standards Mapping (S1410)

Version 3.1

Approved for release

**National E-Health Transition Authority**

**National E-Health Transition Authority Ltd**
Level 25
56 Pitt Street
Sydney, NSW, 2000
Australia.
www.nehta.gov.au

# Document control

| | |
|---|---|
| **Name of document:** | NESAF R3.1 – Standards Mapping |
| **Document owner:** | National E-Health Security and Access Framework |
| **Document coordinator:** | NESAF Configuration Librarian |
| **Author(s):** | NESAF Development Team |
| **Document approver:** | Project Executive |

## Document authoring and review

| Version | Date | Author | Status and nature of amendments |
|---|---|---|---|
| 3.1 | 20120330 | NESAF Team | Version 3.1 Approved for release |

## Document publication

| | |
|---|---|
| **Publication:** | ✓ Internal ✓ External ✓ Public |
| **Published version and date:** | The March 2012 publication of the NESAF has been released for adoption and implementation trials. The NESAF will continue to be developed through application learning's, community feedback and changes to eHealth technologies, International and Australian Standards, as well as changes to the Australian Health working practices. |

This page is intentionally left blank

# Table of contents

This page is intentionally left blank

# 1 Introduction

## 1.1 Purpose

The purpose of this document is to provide initial suggestions for the development of the Standards Mapping document within the National E-Health Security and Access Framework (NESAF) Release 3 (R3.1) suite of documents.

## 1.2 Intended audience

This document is intended for use by the NEHTA National E-Health Security and Access Framework Programme Board to promote discussion and guide further development of the Standard Mapping document within the NESAF R3.1 suite of documents.

## 1.3 Scope

The scope of this document relates to the suite of standards that have been referenced in the development of NESAF R3.1, and/or are considered useful references for readers seeking specific knowledge or guidance in greater depth in relation to areas covered within NESAF R3.1.

## 1.4 Overview

This document provides an illustrated map of primary and secondary standards and relevant frameworks related to NESAF R3.1. A brief description is provided in relation to each of the standards and frameworks in the map.

## 1.5 Questions and feedback

The NESAF Programme values your feedback about the usefulness of this document. We also encourage your comments or suggestions about the content of the standards mapping document. Please direct your questions or feedback to feedback.saf@nehta.gov.au.

# 2 Standards and frameworks

## 2.1 Standards background

The health informatics community in Australia is highly active in the security and access domain. There is a substantial body of contemporary thinking coming from this work that may be applicable in eHealth projects.

Application of standards in eHealth systems is influenced by many factors, and there is often a range of options available when designing and implementing new eHealth services. The choices about which standards are used are sometimes directed by existing systems and vendor capabilities, but there may also be legislative or regulatory requirements which oblige use of standards or services in eHealth projects.

NESAF R2 also leverages content from other recognised frameworks, particularly national frameworks produced by the Australian government. Frameworks such as the Protective Security Policy Framework (PSPF) developed through the Attorney General's Department and the National e-Authentication Framework (NeAF) developed by Australian Government Information Management Office are important for NESAF.

International work done by other healthcare groups are also applicable for NESAF, such as work being developed as part of HL7 Privacy, Access and Security Services (PASS) work program.

Influences on NESAF also come directly from legislation, such as the Commonwealth and state privacy laws. Application of NESAF should encompass necessary measures to ensure that relevant National Privacy Principles or Information Privacy Principles are supported.

## 2.2 Standards and frameworks map

There are three types of standards incorporated into NESAF.

1. **Primary standards** - NESAF is closely aligned to the elements and approach used in these standards.
2. **Secondary standards** - NESAF primary standards may reference these standards, or these standards may provide support to the broader security and access domain covered by NESAF.
3. **Relevant frameworks** - these are relevant technical and policy documents, typically from governments in Australia and overseas.

Figure 1 on the following page provides an overview of the relevant standards and frameworks.

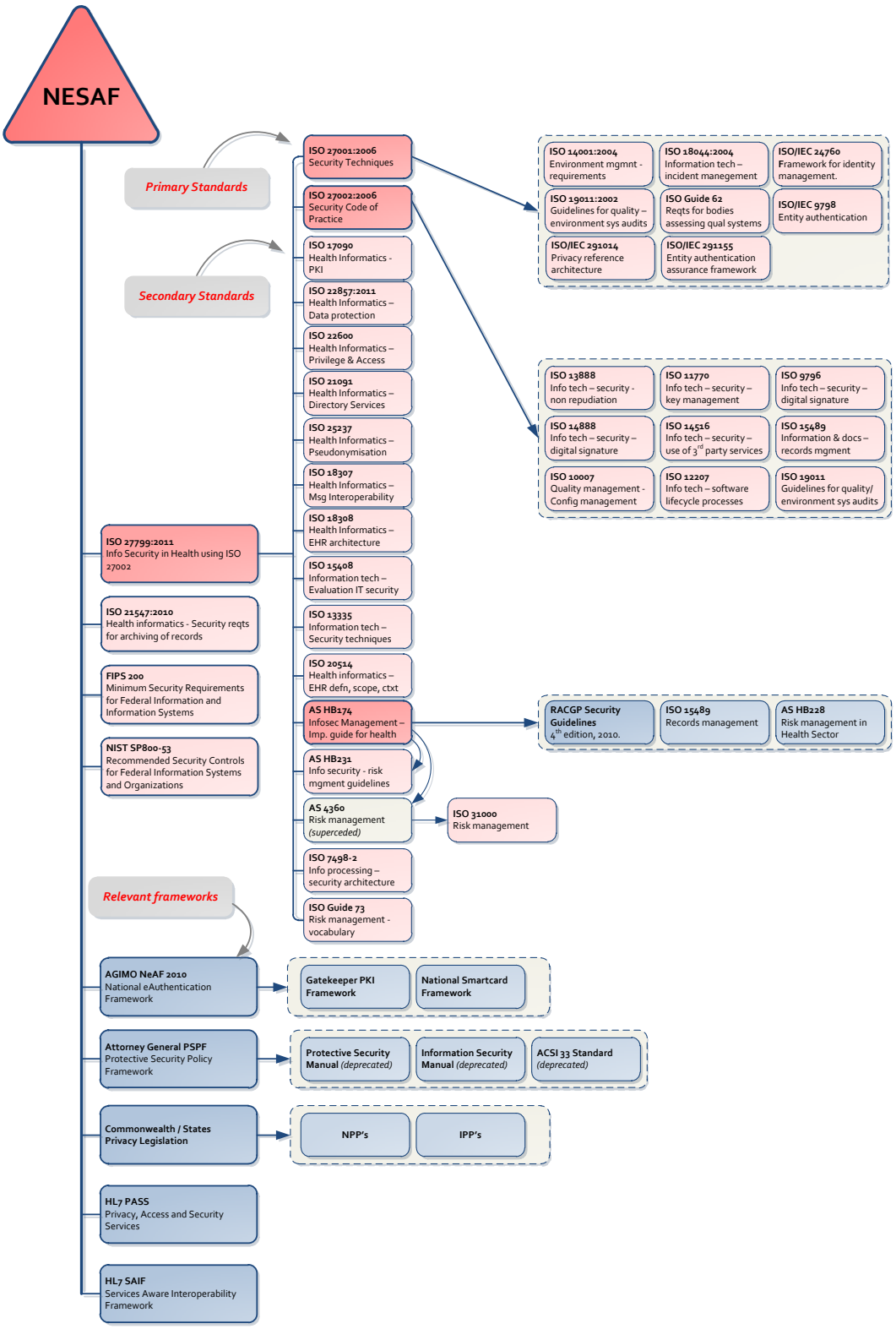


**Figure 1: Standards map**

### 2.2.1 Standards and frameworks descriptions

The following table provides a brief description of the key standards and frameworks referenced in Figure 1.

| Standard/Framework | Description |
|---|---|
| **Primary Standards** | |
| **AS ISO 27799** - Information security management in health using ISO/IEC 27002 | The objective of this standard is to specify guidance on healthcare organisations and other custodians of personal health information on how best to protect the confidentiality, integrity and availability of such information by implementing ISO/IEC 27002 which has been adopted by Standards Australia and Standards New Zealand as AS/NZS ISO/IEC 27002. Specifically, this Australian Standard addresses the special information security management needs of the health sector and its unique operating environments. This Australian Standard is a companion to ISO/IEC 27002.<br><br>The standard specifies a set of detailed controls for managing health information security and provides health information security best practice guidelines. By implementing this standard, healthcare organisations and other custodians of health information will be able to ensure a minimum requisite level of security that is appropriate to their organisation's circumstances and that will maintain the confidentiality, integrity and availability of personal health information.<br><br>The standard applies to health information in all its aspects, whatever form the information takes (words and numbers, sound recordings, drawings, video and medical images), whatever means are used to store it (printing, writing on paper or electronic storage) and whatever means are used to transmit it (by hand, via fax, over computer networks or by post), as the information must always be appropriately protected.<br><br>The standard is intended for those responsible for overseeing health information security and for healthcare organisations and other custodians of health information seeking guidance on this topic, together with their security advisors, consultants, auditors, vendors and third-party service providers. |

| Standard/Framework | Description |
|---|---|
| **ISO/IEC 27001**- Information technology - Security techniques - Information security management systems - Requirements. | The standard provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS).<br><br>The ISMS is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties. It specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the organisation's overall business risks. It specifies requirements for the implementation of security controls customised to the needs of individual organisations or parts thereof.<br><br>The process approach for information security management presented in this International Standard encourages its users to emphasise the importance of:<br>1. understanding an organisation's information security requirements and the need to establish policy and objectives for information security;<br>2. implementing and operating controls to manage an organisation's information security risks in the context of the organisation's overall business risks;<br>3. monitoring and reviewing the performance and effectiveness of the ISMS; and<br>4. continual improvement based on objective measurement.<br><br>This international standard covers all types of organisations (e.g. commercial enterprises, government agencies or non-profit organisations). |
| **ISO/IEC 27002**- Information technology - Security techniques - Code of practice for information security management. | This international standard establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organisation. The objectives outlined in this international standard provide general guidance on the commonly accepted goals of information security management.<br><br>The control objectives and controls in the standard are intended to be implemented to meet the requirements identified by a risk assessment. The international standard provides practical guidelines for developing organisational security standards and effective security management practices and to help build confidence in inter-organisational activities.<br><br>This standard contains 11 security control clauses collectively containing a total of 39 main security categories and one introductory clause introducing risk assessment and treatment. |

| Standard/Framework | Description |
|---|---|
| **Secondary Standards** | |
| **ISO/TS 21547** Technical Specification. Health informatics - Security requirements for archiving of records - Principles. | This technical specification and a complementary Technical Report ISO/TR 21548, concentrate on the security requirements (integrity, confidentiality, availability and accountability) necessary for ensuring adequate protection of health information in long-term digital preservation. This technical specification addresses privacy protection requirements for both the electronic health record (EHR) and an eArchiving system used in the healthcare environment and defines architecture and technology-independent security requirements for the long-term preservation of EHRs.<br><br>The purpose of this technical specification is to define the basic principles needed to securely preserve health records in any format for the long term. There are different architectural and technical ways to develop and implement long-term preservation of electronic health records. Electronic health records are, in many cases, archived in the form of documents, but other technical solutions also exist.<br><br>In this technical specification archiving is understood to be a wider process than just the permanent preservation of selected records. Archiving of EHRs is an holistic process covering records maintenance, retention, disclosure and destruction when the record is not in active use. Archiving also includes tasks the EHR system should perform before the record is sent to the EHR-archive. |
| **FIPS 200** Minimum Security Requirements for Federal Information and Information Systems | The *E-Government Act of 2002 (Public Law 107-347)* recognised the importance of information security to the economic and national security interests of the United States. FIPS Publication 200, is the second of two mandatory security standards required by the *Federal Information Security Management Act (FISMA)* of 2002. It specifies minimum security requirements for information and information systems supporting the executive agencies of the US federal government and a risk-based process for selecting the security controls necessary to satisfy the minimum security requirements. The standard seeks to promote the development, implementation, and operation of more secure information systems within the US federal government by establishing minimum levels of due diligence for information security and facilitating a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems that meet minimum security requirements. |

| Standard/Framework | Description |
|---|---|
| | The minimum security requirements cover seventeen security-related areas with regard to protecting the confidentiality, integrity and availability of federal information systems and the information processed, stored, and transmitted by those systems. The security-related areas include:<br>1. Access control<br>2. Awareness and training<br>3. Audit and accountability<br>4. Certification, accreditation, and security assessments<br>5. Configuration management<br>6. Contingency planning<br>7. Identification and authentication<br>8. Incident response<br>9. Maintenance<br>10. Media protection<br>11. Physical and environmental protection<br>12. Planning<br>13. Personnel security<br>14. Risk assessment<br>15. Systems and services acquisition<br>16. System and communications protection<br>17. System and information integrity<br>The seventeen areas represent a broad-based, balanced information security program that addresses the management, operational, and technical aspects of protecting federal information and information systems. |

| Standard/Framework | Description |
|---|---|
| **NIST SP800-53** Recommended Security Controls for Federal Information Systems and Organizations | Provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the US federal government to meet the requirements of FIPS 200, Minimum Security Requirements for Federal Information and Information Systems. The guidelines apply to all components of an information system that process, store, or transmit federal information. The guidelines have been developed to help achieve more secure information systems and effective risk management within the federal government by:<br>• Facilitating a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems and organisations.<br>• Providing a recommendation for minimum security controls for information systems categorized in accordance with FIPS 199, Standards for Security Categorization of Federal Information and Information Systems.<br>• Providing a stable, yet flexible catalogue of security controls for information systems and organizations to meet current organisational protection needs and the demands of future protection needs based on changing requirements and technologies.<br>• Creating a foundation for the development of assessment methods and procedures for determining security control effectiveness.<br>• Improving communication among organisations by providing a common lexicon that supports discussion of risk management concepts. |
| **ISO 17090** Health Informatics: Public key infrastructure | ISO 17090 describes the common technical, operational and policy requirements that need to be addressed to enable digital certificates to be used in protecting the exchange of healthcare information within a single domain, between domains and across jurisdictional boundaries. Its purpose is to create a platform for global interoperability. It specifically supports digital certificate-enabled communication across borders, but could also provide guidance for the national or regional deployment of digital certificates in healthcare.<br>ISO 17090 consists of the following parts, under the general title Health informatics — Public key infrastructure:<br>• Part 1: Overview of digital certificate services - defines the basic concepts underlying the use of digital certificates in healthcare and provides a scheme of interoperability requirements to establish digital certificate-enabled secure communication of health information. |

| Standard/Framework | Description |
|---|---|
| | • Part 2: Certificate profile - gives a brief introduction to public key cryptography and the basic components needed to deploy digital certificates in healthcare. It specifies the certificate profiles required to interchange healthcare information within a single organization, between different organizations and across jurisdictional boundaries.<br>• Part 3: Policy management of certification authority - deals with management issues involved in implementing and using digital certificates in healthcare. It identifies the principles needed in a healthcare security policy for cross border communication. It also defines the minimum levels of security required, concentrating on the aspects unique to healthcare. |
| **ISO 22857** Health Informatics: Guidelines on data protection to facilitate trans-border flows of personal health information | This International Standard aims to facilitate international health-related applications involving the transfer of personal health data. It seeks to provide the means by which data subjects, such as patients, may be assured that health data relating to them will be adequately protected when sent to, and processed in, another country.<br>ISO 22857 provides guidance on data protection requirements to facilitate the transfer of personal health data across national borders. The standard covers both the data protection principles that should apply to international transfers and the security policy which an organisation should adopt to ensure compliance with those principles. |
| **ISO/TS 22600** Health informatics: Privilege Management and Access Control | This Technical Specification defines privilege management and access control services required for communication and use of distributed health information over domain and security borders.<br>ISO/TS 22600 consists of the following parts, under the general title Health informatics — Privilege management and access control:<br>• Part 1: Overview and policy management - describes the scenarios and the critical parameters in cross border information exchange. It also gives examples of necessary documentation methods as the basis for the policy agreement.<br>• Part 2: Formal models - describes and explains, in more detail, the architectures and underlying models for the privileges and privilege management, which are necessary for secure information sharing plus examples of policy agreement templates.<br>• Part 3: Implementations - describes examples of implementable specifications of application security services and infrastructure services using different specification languages. |

| Standard/Framework | Description |
|---|---|
| **ISO/TS 21091** Technical Specification. Health informatics: Directory services for security, communications and identification of professionals and patients. | This technical specification defines minimal specifications for directory services for health care using the X.500 framework. The specification provides the common directory information and services needed to support the secure exchange of health care information over public networks. It supports directory services aiming to support identification of health professionals and organisations and the patients/consumers (sometimes referred to as master patient indices). |
| ISO/TS 25237 Technical Specification. Health informatics: Pseudonymization | This technical specification provides a conceptual model of the problem areas, requirements for trustworthy practices, and specifications to support the planning and implementation of pseudonymisation services. De-identification is the general term for any process of removing the association between a set of identifying data and the data subject. Pseudonymisation is a subcategory of de-identification. The pseudonym is the means by which pseudonymised data are linked to the same person across multiple data records or information systems without revealing the identity of the person. Pseudonymisation can be performed with or without the possibility of re-identifying the subject of the data (reversible or irreversible pseudonymisation).<br><br>This technical specification also defines the interfaces to pseudonymisation services to ensure interoperability between pseudonymisation service systems, identity management systems, information providers and recipients of pseudonyms. It contains principles and requirements for privacy protection using pseudonymisation services for the protection of personal health information. |
| **ISO/TR 18307** Technical Report. Health informatics: Interoperability and compatibility in messaging and communication standards - Key characteristics. | This technical report describes a set of key characteristics to achieve interoperability and compatibility in trusted health information interchange between communicant application systems.<br><br>The key characteristics describe inter-application interoperability needs of the healthcare community, in particular the subject of care, the healthcare professional/caregiver, the healthcare provider organization, its business units and the integrated delivery network.<br><br>The key characteristics offer criteria for standards developers and implementers of standards for messaging and communications in the healthcare domain and provide a guide for software developers and vendors, healthcare providers and end users. |

| Standard/Framework | Description |
|---|---|
| **AS ISO 18308** Australian Standard Health Informatics: Requirements for an electronic health record architecture | The purpose of this technical specification is to assemble and collate a set of clinical and technical requirements for an electronic health record architecture (EHRA) that supports using, sharing, and exchanging electronic health records across different health sectors, different countries, and different models of healthcare delivery. This Technical Specification gives requirements for the architecture but not the specifications of the architecture itself. |
| **ISO 15408** Information Technology: Evaluation IT Security | ISO/IEC 15408 in its entirety is meant to be used as the basis for evaluation of security properties of IT products.<br>• Part 1 - ISO/IEC 15408-1 establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts. It establishes the core concept of a Target of Evaluation (TOE); the evaluation context; and describes the audience to which the evaluation criteria are addressed. An introduction is provided to the basic security concepts necessary for evaluation of IT products.<br>• Part 2 - ISO/IEC 15408-2 defines the content and presentation of the security functional requirements to be assessed in a security evaluation using ISO/IEC 15408. It contains a comprehensive catalogue of predefined security functional components that will meet most common security needs of the marketplace.<br>• Part 3 - ISO/IEC 15408-3 defines the assurance requirements of the evaluation criteria. |
| **AS 13335** Information Technology: Guidelines for the management of IT Security | This Australian Standard contains guidance on the management of IT security. The Standard is published in five parts as follows:<br>• Part 1: Concepts and models for IT Security<br>• Part 2: Managing and planning IT Security<br>• Part 3: Techniques for the management of IT Security<br>• Part 4: Selection of safeguards<br>• Part 5: Management guidance on network security |

| Standard/Framework | Description |
|---|---|
| **ISO/TR 20514** Technical Report. Health Informatics - Electronic health record - definition, scope and context | This technical report describes a classification of electronic health records, provides simple definitions for the main categories of EHR and provides supporting descriptions of the characteristics of electronic health records and record systems. this report was prepared to describe the scope of application of the family of EHR standards currently programmed for development by ISO.<br><br>The primary purpose of ISO's family of EHR standards is to maximize interoperability between electronic records and systems that are specifically intended to be shareable, irrespective of the technologies they use and the platforms on which they reside. |
| **AS HB174** Handbook. Information Security Management-Implementation guide for the health sector. | The purpose of this guide is to interpret AS/NZS 17799:2001-Information Technology – Code of Practice for Information Security Management, and apply this standard specifically to the interests and unique information security requirements of the Australian health sector. The handbook provides a set of detailed controls, which describe best practices in information security. The handbook was developed to address the special considerations that are required for the health sector, with particular emphasis on individuals and small to medium sized health practitioners. The guide is designed to appeal to health professionals and non-computing professionals to ensure that it is clear, concise and easy to understand and interpret. The content is therefore not of a highly technical nature.<br><br>The intention of this handbook is that it is to be used as a document for the initiation, implementation and maintenance of information security measures within a health business. |
| **AS HB231** Handbook. Information Security - Risk management guidelines | This handbook provides a generic guide for the establishment and implementation of a risk management process for information security risks.<br><br>AS/NZS ISO/IEC 17799 establishes a code of practice for selecting information security controls (or equivalently treating information security risks). AS/NZS 7799.2 (BS 7799.2) specifies an information security management system. Both documents require that a risk assessment process is used as the basis for selecting controls (treating risks). This Handbook complements these standards by providing additional guidance concerning management of information security risks.<br><br>The guidance in this handbook is not intended to be a comprehensive schedule of information security threats and vulnerabilities. It is intended to serve as a single reference point describing an information security risk management process suitable for most situations encountered in industry and commerce and therefore can be applied by a wide range of organizations. |

| Standard/Framework | Description |
|---|---|
| **ISO 31000:2009** Risk Management - Principles and Guidelines | This international standard provides principles and generic guidelines on risk management. It establishes a number of principles that need to be satisfied to make risk management effective. The standard recommends that organizations develop, implement and continuously improve a framework whose purpose is to integrate the process for managing risk into the organisation's overall governance, strategy and planning, management, reporting processes, policies, values and culture.<br><br>This international standard can be used by any public, private or community enterprise, association, group or individual. Therefore, this international standard is not specific to any industry or sector. It can be applied throughout the life of an organization, and to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets.<br><br>It is intended that this international standard be utilized to harmonise risk management processes in existing and future standards. It provides a common approach in support of standards dealing with specific risks and/or sectors, and does not replace those standards. |
| **ISO 7498-2** Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security architecture | This international standard provides a general description of security services and related mechanisms. It extends the field of application of ISO 7498 to cover secure communications between open systems by adding to (but not modifying) the concepts and principles included in ISO 7498. It is not an implementation specification, nor a basis for assessing the conformance of actual implementations. |
| **ISO Guide 73** Risk Management - Vocabulary | This guide provides basic vocabulary to develop a common understanding of risk management concepts and terms among organisations and functions, and across different applications and types. It aims to encourage a mutual and consistent understanding of, and a coherent approach to, the description of activities relating to the management of risk, and the use of uniform risk management terminology in processes and frameworks dealing with the management of risk.<br><br>For principles and guidelines on risk management, reference is made to ISO 31000. |

| Standard/Framework | Description |
|---|---|
| ISO/IEC 24760 Information technology - Security techniques - A framework for identity management. | Data processing systems commonly gather a range of information on their users, be it a person, piece of equipment, or piece of software connected to them, and make decisions based on the gathered information. Such identity-based decisions may concern access to applications or other resources.<br><br>To address the need to efficiently and effectively implement systems that make identity-based decisions, ISO/IEC 24760 specifies a framework for the issuance, administration, and use of data that serves to characterize individuals, organizations or information technology components which operate on behalf of individuals or organizations.<br><br>ISO/IEC 24760 specifies fundamental concepts and operational structures of identity management with the purpose to realize information system management so that information systems can meet business, contractual, regulatory and legal obligations. |
| ISO/IEC 9798 (all parts), Information technology - Security techniques - Entity authentication. | An authentication model and general requirements and constraints for entity authentication mechanisms which use security techniques. These mechanisms are used to corroborate that an entity is the one that is claimed. An entity to be authenticated proves its identity by showing its knowledge of a secret. The mechanisms are defined as exchanges of information between entities and, where required, exchanges with a trusted third party.<br><br>The details of the mechanisms and the contents of the authentication exchanges are given in subsequent parts of ISO/IEC 9798. |

| Standard/Framework | Description |
|---|---|
| **Relevant Frameworks** | |
| **AGIMO National e-Authentication Framework** (NeAF) 2008 | The framework is endorsed by the Australian Online and Communications Council, which operates as the peak ministerial forum across Australia on strategic approaches to information and communications technology issues.<br><br>The National e-Authentication Framework (NeAF) is intended to assist agencies, jurisdictions and sectors in authenticating the identity of the other party to a desired level of assurance or confidence. The NeAF encompasses the electronic authentication (e-Authentication) of the identity of individuals and businesses dealing with the government, on one side of the transaction, as well as the authentication of government websites on the other side.<br><br>The National Framework provides guidance on models for the implementation of e-Authentication solutions and planning standards for website authentication. Adoption of the NeAF across all tiers of government is intended to minimise duplication of effort and achieve consistency of authentication approaches within and across jurisdictional boundaries. This will maximise the efficiency and effectiveness of electronic service delivery by Australian government jurisdictions as well as providing scope for reducing the costs to the community of interacting electronically with government. |
| **Attorney General: Protective Security Policy Framework** | The Protective Security Policy Framework (PSPF) sets out the Australian government policy and guidance on protective security. Protective security is a combination of procedural, physical, personnel, and information security measures designed to provide government information, functions, resources, employees and clients with protection against security threats.<br><br>The PSPF applies to government agencies and any organisations working on behalf of, or handling Australian government information and assets. This may include other governments, and contract service or goods providers. The framework supports agencies in implementing the government's protective security policy.<br><br>Protective security policies differ according to the range of business and security risks faced by each agency, however, the minimum security requirements are mandatory for all agencies. Compliance with mandatory requirements provides assurance needed for the secure sharing of information across government. |
| **Commonwealth/State Privacy Legislation** | The *Privacy Act 1988 (Cth)* applies to Commonwealth and ACT government agencies and all private health providers. |

| Standard/Framework | Description |
|---|---|
| | • Commonwealth and ACT government health providers need to comply with the *Privacy Act's* Information Privacy Principles.<br>• All private health providers, regardless of size, must comply with the *Privacy Act's* National Privacy Principles.<br>• Some private health providers in NSW, Victoria and ACT are also bound by jurisdictional privacy principles.<br>• Most state and territory public health providers are governed by different, though similar, privacy principles on data security, access, use and disclosure and anonymity. |
| **HL7 Privacy, Access and Security Services (PASS)** | Currently in development.<br>Phase 1 PASS-Alpha services are intended to provide the basic capabilities that allow a patient or provider to request access to patient health information from a protected resource and, based upon the security and privacy policies applied by the resource, have that access granted or denied. This phase will focus on the following:<br>– Create an overall PASS Architecture Framework<br>– Create conceptual, platform independent and platform specific level standards for: Access Control; Federated Identity; Audit; and Consumer Preferences<br>– Identify or develop vocabularies in support of the PASS-Alpha subproject specifications.<br>– Basic functionality in some real world scenarios based on core use case scenarios. |
| **HL7 Services Aware Interoperability framework (SAIF)** | The HL7 SOA-Aware Interoperability Framework provides a set of constructs, best practices and processes and that enable HL7 specifications to achieve cross-specification consistency across a range of interoperability paradigms, e.g. messages, documents, or services. |