nehta

National eHealth Security & Access Framework (NESAF) v4.0

Framework Model and Controls v1.0

6 June 2014

Approved for external use

Document ID: NEHTA-1549:2014

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 information

Key information

Owner	Lead Security Architect
Date of next review	2 June 2015
Contact for enquiries	NEHTA Help Centre t: 1300 901 001 e: help@nehta.gov.au

Product version history

NESAF version	Product version	Date	Release comments
2.0		29 Jul 2011	Version 2.0 Approved for release
3.0		30 Nov 2011	Version 3.0 Approved for release
3.1		30 Mar 2012	Version 3.1 Approved for release
4.0	1.0	06 Jun 2014	See NESAF v4.0 release note for details

Table of contents

Table of figures

1 Introduction

1.1 Purpose

This document describes in detail the security controls recommended in the NESAF. By implementing the controls within this document, healthcare organisations will be able to ensure that a minimum level of security is in place appropriate to their organisation's circumstances and be assured that the confidentiality, integrity and availability of patients' personal health information is maintained.

1.2 Intended audience

This document is for IT professionals responsible for overseeing information security, or involved in specifying, designing and building security controls for their healthcare organisation.

People unfamiliar with the NESAF should read the *NESAF v4.0 Overview* [1] first.

1.3 Document map

This document is a part of a suite of documents designed to provide specific views of the NESAF for different audiences, that is, general, business, and technical, as illustrated below.

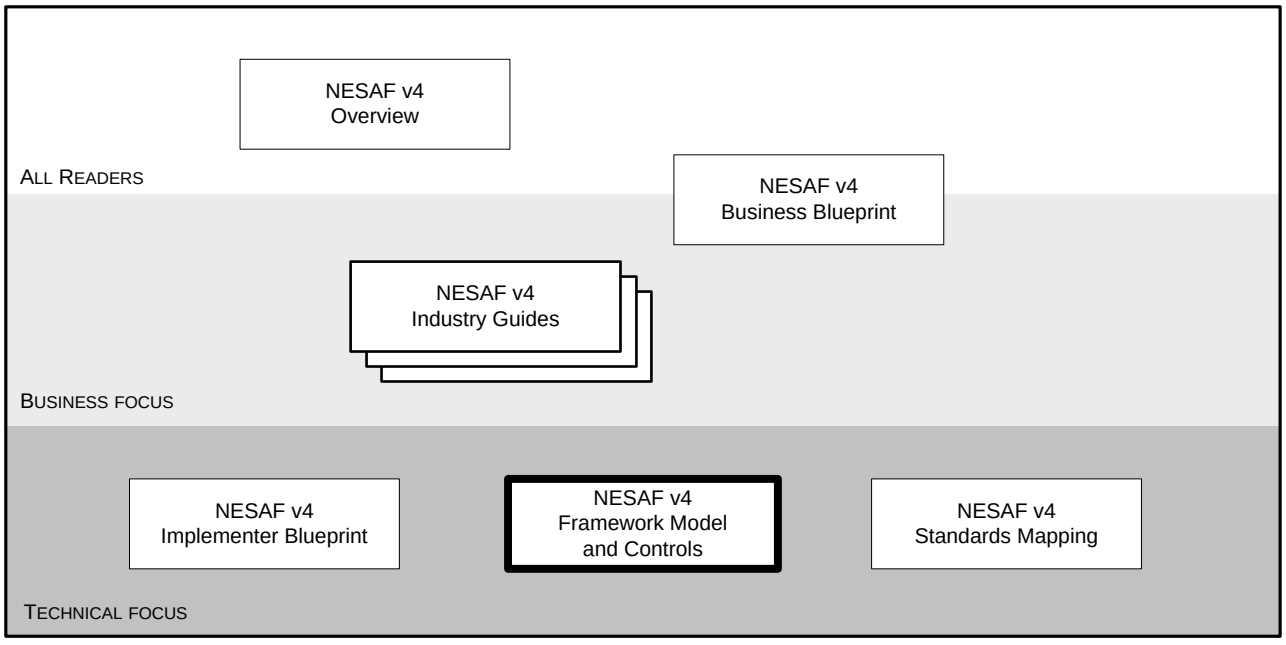

Figure 1: NESAF v4.0 document map

As this map would suggest, all readers with an interest in the NESAF should read both the *NESAF v4.0 Overview* [1] and the *NESAF v4.0 Business Blueprint* [2]. Once these two documents have been absorbed, readers should be well placed to judge which of the other NESAF documents are most relevant to their needs. See Section 1.5 for additional details.

1.4 Scope

The 11 security controls described in this document are based on standards such as *ISO/IEC 27002:2005* [3] and *AS ISO 27799-2011* [4]. These controls are intended to mitigate the risks identified during the assessment of your organisation using the patterns in the *NESAF v4.0 Implementer Blueprint* [5].

Moreover, the controls contained within this document can be applied to health information in all its different forms to be created, stored or transmitted. For example, the controls may be applied to sound recordings, text, video or medical images, as well as electronic or paper-based storing methods and transmission mechanisms, such as facsimile, computer networks or by post.

1.5 The NESAF document pyramid

The pyramid diagram below depicts the major themes and relationships of the NESAF, also noting the documents that address those themes. Introductory documents are closer to the apex, and the technical foundations are closer to the base. At the core of the NESAF is its risk-based approach, with the ultimate goal of creating systems that can be trusted by clinicians and users alike.

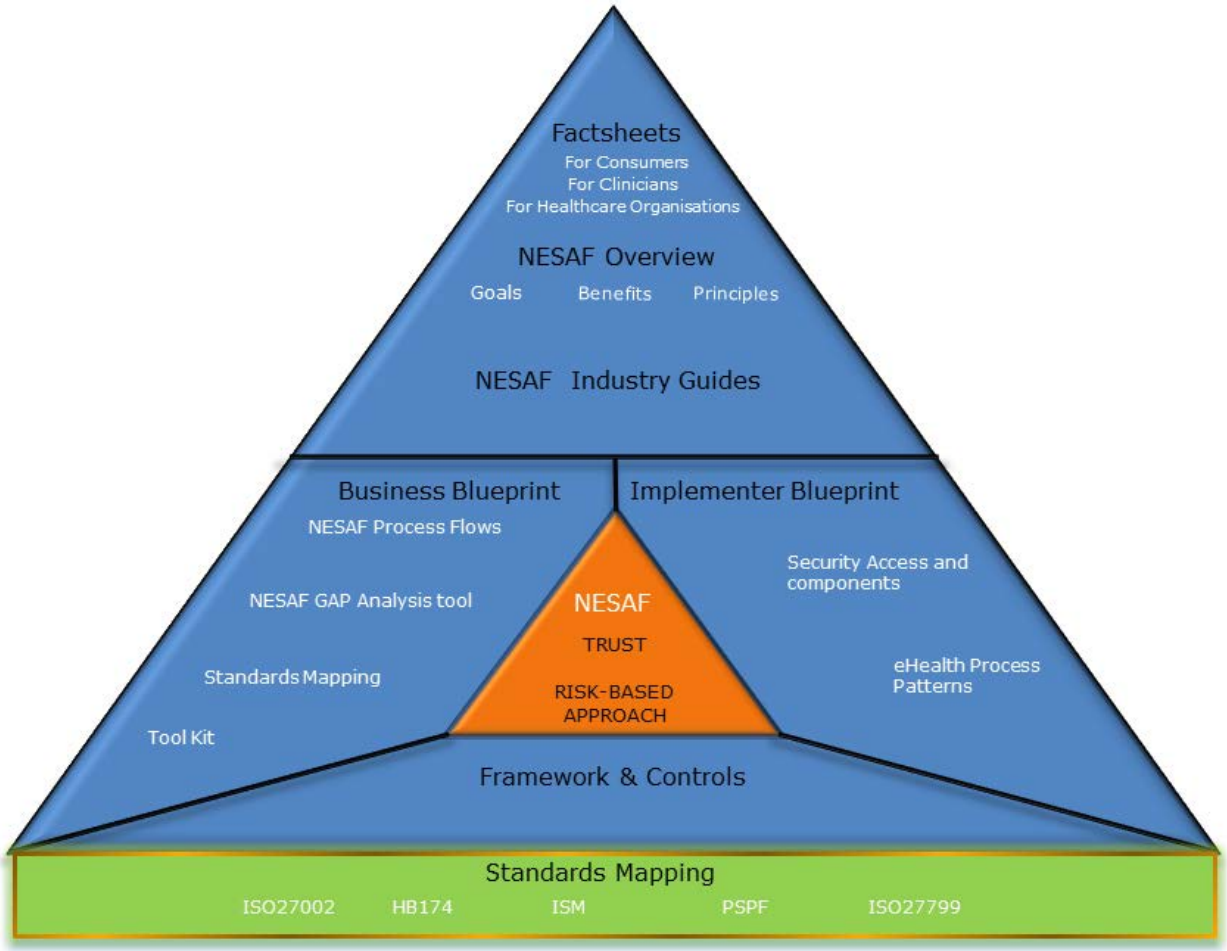

Figure 2: NESAF themes and documents

The following table elaborates on the documentation depicted above.

Table 1: NESAF documentation details

Document	Intended Audience	Description
NESAF v4.0 Consumer Factsheet [6]	General public	An introduction to the NESAF 4.0, targeted at the general public.
NESAF v4.0 Clinician Factsheet [7]	Clinicians	An introduction to the NESAF 4.0, targeted at clinicians.
NESAF v4.0 Healthcare Organisation Factsheet [8]	Healthcare organisations	An introduction to the NESAF 4.0, targeted at healthcare organisations.
NESAF v4.0 Overview [1]	Business oriented document, suitable for the following: • Business executives • System owners • Healthcare organisation management teams	Provides a holistic view of the NESAF and its goals, benefits and principles.
NESAF Industry Guides (in development)	• Administrators • Clinicians • Health information managers • Implementers • Security Practitioners • Users	Security guidance for healthcare organisations, focussing on particular strategies or technologies.
NESAF v4.0 Business Blueprint [2]	• Business executives • System owners • Healthcare organisation management teams	This document aids the business to analyse the risk and identify appropriate security methods. Provides details of NESAF process flows and access to tool kits that can be utilised in implementing the NESAF.
NESAF v4.0 Implementer Blueprint [5]	Technically-oriented document aimed at ICT professionals.	Provides technical information on how ICT professionals can implement the NESAF. It introduces the eHealth process patterns and the security and access components to assist in the completion of a risk-based approach to information security.
NESAF v4.0 Framework Model and Controls [9] (this document)	ICT professionals	Describes a standards-based model and relevant industry standards, including ISO27799 and ISO27001. This document identifies 11 key security and access control areas. Within each area a range of controls are identified that businesses may select, based on the outcome of risk assessment processes to address the security and access requirements for their organisation.
NESAF v4.0 Standards Mapping [10]	• Business executives • ICT professionals	A suite of standards that have been referenced or mapped in the development of NESAF v4.0, which may provide useful references for readers seeking a deeper understanding of the areas covered within NESAF v4.0.

1.6 Overview

The framework model is based on Australian Standards for information security management and information security management in health[1], and has been tailored to address the specific health information security and access requirements in the Australian eHealth environment.

The NESAF takes a risk-based approach to information security. It assists organisations in the Australian eHealth environment to identify and assess risks that may affect their organisations. The controls described in this document provide organisations with guidance to select and enforce controls that will mitigate the risks that have been identified through a risk assessment.

The NESAF identifies eleven key security and access areas (for example, Access control (Control Area G)) relating to eHealth, each of which contains one or more control categories (for example, Requirements for access control in health (G.1), User access management (G.2)). Each control category contains a control objective stating what is to be achieved, and one or more controls that can be applied to achieve the control objective.

[1] Specifically, *ISO/IEC 27002:2005* [3] and *AS ISO 27799-2011* [4].

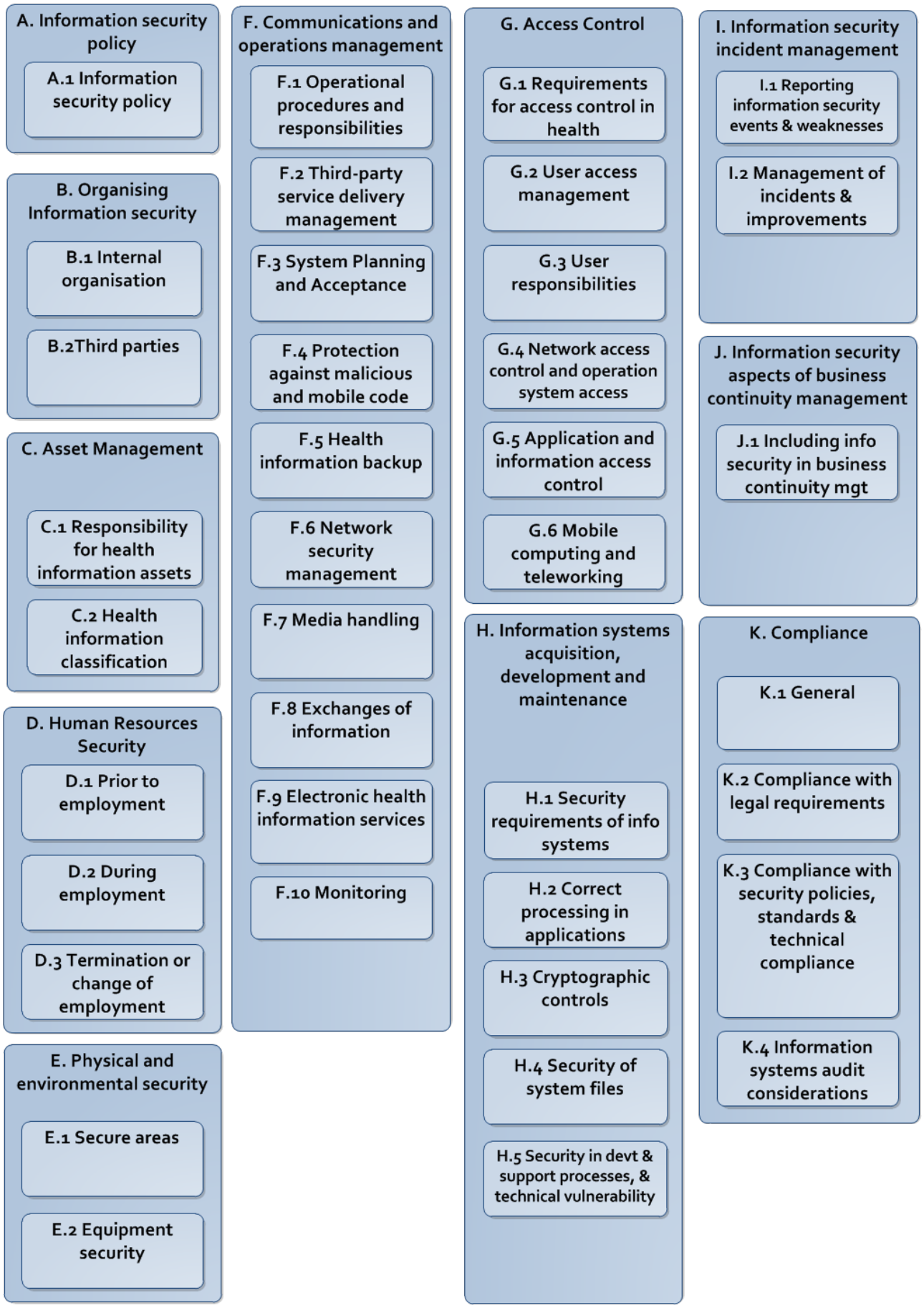

Figure 3: Standards-based framework model

The majority of control categories, control objectives and controls contained in the following tables have been derived directly from *ISO/IEC 27002:2005* [3] and *AS ISO 27799-2011* [4], with some additional controls identified during the development of NESAF Version 1.[2]

1.7 Using this document

This document provides a detailed description of each control within the NESAF. It gives a unique reference number for each control, notes the control category, gives detailed wording for each control and also attributes the source of the control back to a recognised standard or framework.

This level of detail allows complete transparency of where the guidance in the control has been sourced. The figure below shows the template used.

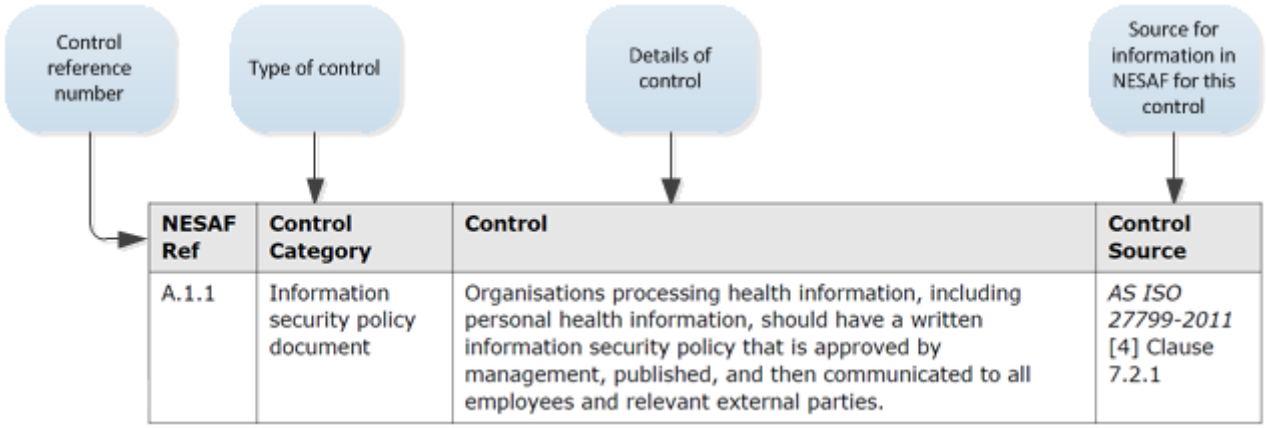

Figure 4: Template map

To accompany the core detail on each control, additional supporting information is also provided. The type of control is categorised, the usage of each control is noted, and the responsibility for each control is noted.

Some controls in the NESAF only have a single entry for each area; others span multiple entries. The value of the table is that it can help to scope an implementation planning study by broadly identifying the areas in the business that will be responsible for each control selected for use in the organisation.

Each control also has notes around implementation. These notes are intended to add some further detail around the types of issues that may be encountered when implementing the control, and can also note other sources for information for organisations to seek out.

Figure 5 below shows the general matrix view of the supporting information, and describes the usage of each of the cells.

[2] For example, F.10.2, H.2.3, and H.2.7.

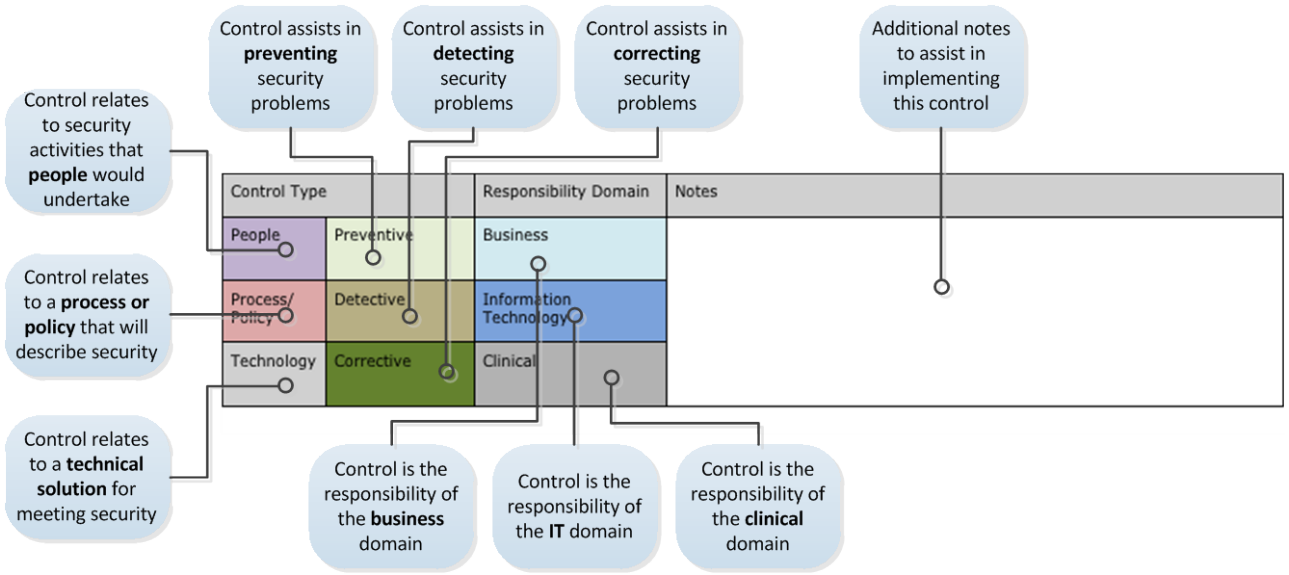

Figure 5: Template colour key

1.8 Questions and feedback

The NESAF programme values your feedback about the usefulness of this document. Please direct your questions, comments and feedback to help@nehta.gov.au .

2 Information security policy (Control Area A)

2.1 Information security policy (A.1)

Control Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

NESAF Ref	Control Category	Control	Control Source
A.1.1	Information security policy document	Organisations processing health information, including personal health information, should have a written information security policy that is approved by management, published, and then communicated to all employees and relevant external parties.	*AS ISO 27799-2011* [4] Clause 7.2.1

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Business Information Technology	Security policies are the foundation of a business's security infrastructure. They provide direction and support for health information security; identify the security and access controls that will be implemented in the organisation at a high level, and serve as a point of reference for all staff in relation to their information security responsibilities, for example, the PCEHR Rules require healthcare provider organisations to have written policies that address security requirements, such as policies for access control mechanisms. Guidance for developing an information security and access policy is included in the *NESAF v4.0 Business Blueprint* [2]. This includes principles for developing security and access policies; suggested contents; specific considerations and comments on the importance of communication of the policy within an organisation.

NESAF Ref	Control Category	Control	Control Source
A.1.2	Review of the information security policy document	The health organisation's information security policy should be subject to ongoing, staged review such that the totality of the policy is addressed at least annually. The policy should also be reviewed when any material new or changed risks are identified, and also after the occurrence of a serious security incident.	*AS ISO 27799-2011* [4] Clause 7.2.2

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Business Information Technology	Changes made to the organisation, ICT systems or other internal or external factors that may affect the organisation's risk profile may need to be reflected in the policy. Reviews of the usefulness of the policy (through reviews or regular feedback) should be undertaken and changes made where required.

3 Organising information security (Control Area B)

3.1 Internal organisation (B.1)

Control Objective: To manage information security within the organisation.

NESAF Ref	Control Category	Control	Control Source
B.1.1	Management commitment to information security, information security coordination and allocation of information security responsibilities	Organisations should: • Clearly define and assign information security responsibilities. • Have an Information Security Management Forum in place to ensure that there is clear direction and visible management support for security initiatives involving the security of health information. At a minimum, organisations should have at least one individual responsible for health information security within the organisation. The health information security forum should meet regularly, on a monthly or near-to-monthly basis. A formal scope statement should be produced that defines the boundary of compliance activity in terms of people, processes, places, platforms and applications.	*AS ISO 27799-2011* [4] Clause 7.3.2.1

Control Type		Responsibility Domain	Notes
People Process/ Policy	Preventive	Business	Responsibilities for information security governance and operations should be clearly documented within the information security policy. Some health organisations may assign specific positions for managing information security, while it is expected that smaller organisations may assign a role to an existing position. Organisations should seek guidance and support from qualified external information security experts as required. See the *NESAF v4.0 Business Blueprint* [2] for a sample of Role Descriptions within a health organisation.

NESAF Ref	Control Category	Control	Control Source
B.1.2	Authorisation process for information processing facilities	A management authorisation process for new information processing facilities should be defined and implemented.	*ISO/IEC 27002:2005* [3] Clause 6.1.4

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Business	All new ICT systems within a health organisation should be authorised by an approved management representative. This representative should be appointed and documented as part of the delegation of information security responsibilities. An authorisation process should be implemented and all staff made aware of this. Each authorisation should be documented and approved prior to connection of any new system, including personal devices.

NESAF Ref	Control Category	Control	Control Source
B.1.3	Confidentiality agreements	Organisations should have a confidentiality agreement in place that specifies the confidential nature of health information. The agreement should be applicable to all personnel accessing health information, including any third parties that have been contracted to provide a service to the health organisation.	*AS ISO 27799-2011* [4] Clause 7.3.2.3

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Business	Managers should ensure that all employees and third parties who may access health or personal information as part of their job sign confidentiality agreements and are aware of the consequences resulting from a breach of the agreement or the information security policy. Agreements should include, but not be limited to: • Definition of the information to be protected (for example, all patient information). • Duration and termination of agreement (the confidentiality requirement extends indefinitely after the agreement termination). • Responsibilities of the signatories to the agreement. • Permitted use of information protected under the agreement. • The right to audit and monitor the signatory's access to the protected information. **Note:** Clause 3.3.2 of the *RACGP security standards and templates* [11] contains a sample Confidentiality Agreement. (Refer also to *ISO/IEC 27002:2005* [3], Clause 6.1.5.)

NESAF Ref	Control Category	Control	Control Source
B.1.4	Contact with authorities, contact with special interest groups	Appropriate contacts with relevant authorities should be maintained. Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained, for example, the RACGP.	*ISO/IEC 27002:2005* [3], Clauses 6.1.6 and 6.1.7.

Control Type		Responsibility Domain	Notes
People	Preventive	Business	Organisations should have procedures in place that specify when and by whom authorities (for example, law enforcement, fire department, supervisory authorities, relevant Privacy or Health Services Commissioners) should be contacted, and how information security incidents should be reported in a timely manner if it is suspected that laws may have been breached. Channels with external, reputable user groups (for example, the Australian Information Security Association) should be established by the person responsible for information security within an organisation so as to stay up to date with relevant information security practices. External, reputable information security sources should be used for information on current vulnerabilities and patches (for example, vendors or AusCERT).
Process/ Policy		Information Technology	

NESAF Ref	Control Category	Control	Control Source
B.1.5	Independent review of information security	The organisation's approach to managing information security and its implementation (that is, control objectives, controls, policies, processes, and procedures for information security) should be reviewed independently at planned intervals, or when significant changes to the security implementation occur.	*ISO/IEC 27002:2005* [3] Clause 6.1.8

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Business	The review may be by an external information security assessor, the organisation's internal audit function or other party not directly involved with the information security function. The review should be documented and a report provided to the person responsible for the organisation's information security, with recommendations on any improvements that need to be made.
		Information Technology	

3.2 Third parties (B.2)

Control Objective: To maintain the security of the organisation's information and information processing facilities that are accessed, processed, communicated to, or managed by third parties.

NESAF Ref	Control Category	Control	Control Source
B.2.1	Identification of risks related to external parties	Organisations processing health information should assess the risks associated with access by external parties to these systems or the data they contain, and then implement security controls that are appropriate to the identified level of risk and to the technologies employed.	*AS ISO 27799-2011* [4] Clause 7.3.3.1

Control Type		Responsibility Domain	Notes
Technology Process/ Policy	Preventive	Business Information Technology	The risks of giving external, often untrusted, external parties access to health information should be identified so that the organisation can implement appropriate protection mechanisms. Importantly, an assessment of any "cloud" or other externally hosted service should be undertaken, as there may be legislative restrictions on the hosting of information – for example, the *Information Security Manual* [12] recommends that organisations implementing processing facilities should be located in Australia or not allow information to leave Australian borders unless approved. Furthermore, Australian Privacy Principle 8 requires entities including healthcare organisations to take steps to ensure that the overseas recipient does not breach the Australian Privacy Principles in relation to the personal information. It is important to note also that an Australian entity may be held liable for any acts done by the overseas recipient which breach the Privacy Act and its Australian Privacy Principles. **Note:** Some guidance on the risk-based approach is given in the *NESAF v4.0 Business Blueprint* [2].

NESAF Ref	Control Category	Control	Control Source
B.2.2	Addressing security when dealing with third parties	All identified security requirements should be addressed before giving third parties access to the organisation's information or assets.	*ISO/IEC 27002:2005* [3] Clause 6.2.2

Control Type		Responsibility Domain	Notes
People Process/ Policy Technology	Preventive	Business Information Technology	Risks assessed when third parties (including customers, vendors, integrators) request access to information or when information is hosted externally (refer to B.2.1) should be treated before any access is granted. Specific considerations should include, but not be limited to: • Description of the reason for the access. • Ensuring third parties only receive access to that which they require and no more. • Access control methods. • Responsibilities for support (included in Service Level Agreements). • Agreements (such as confidentiality and consequences for breaching agreements). • Identification of external users. • Auditing of third party access. An efficient method of providing access to third parties may be to group like third parties together and develop procedures and protocols for implementing access for members of that group.

NESAF Ref	Control Category	Control	Control Source
B.2.3	Addressing security in third-party agreements	Health organisations using the services of third parties, where the services of those parties process personal health information, should employ formal contracts that specify: • The relevant privacy laws that apply to the health organisation and in turn the third party as its service provider, and the requirement to uphold these privacy laws. The confidential nature and value of the personal health information should likewise be specified. • The security measures to be implemented and/or complied with. • Limitations to access to these services by third parties. • The service levels to be achieved in the services provided. • The format and frequency of reporting to the health organisation's Information Security Management Forum. • The arrangement for representation of the third party in appropriate health organisation meetings and working groups. • The arrangements for compliance auditing of the third parties. • The consequences exacted in the event of any failure in respect of the above. • If the third party is located off-shore and personal health information will be disclosed overseas, for the third party to comply with *Privacy Act 1988 (Cth)* [13] in its processing of the personal health information.	*AS ISO 27799-2011* [4] Clause 7.3.3.3

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Business	Consider terminating the agreement with the third party provider if security failures cannot be contained with penalties. **Note:** The entire information lifecycle as it transitions from creation through to deletion should be considered in this context.

4 Asset Management (Control Area C)

4.1 Responsibility for health information assets (C.1)

Control Objective: To achieve and maintain appropriate protection of organisational assets.

NESAF Ref	Control Category	Control	Control Source
C.1.1	Responsibility for health information assets	Organisations processing personal health information should: • account for health information assets (inventory); • have a designated custodian of these health information assets; and: • have rules for acceptable use of these assets that are identified, documented, and implemented.	*AS ISO 27799-2011* [4] Clause 7.4.1

Control Type		Responsibility Domain	Notes
People	Preventive	Business	Information assets describe any information, or collection of information, which has value to the organisation. An information asset in a health organisation may include, but not be limited to: • Patient database • IT hardware • Internet connection software • Medical devices • Staff information • Drug database • Payroll information The information asset custodian is the person responsible for overseeing and implementing the necessary safeguards to protect the information assets, at the level classified by the information owner. In a large clinic the information asset custodian may be the IT manager while the information owners would be the health practitioners. Health organisations should have rules (including responsibilities) for maintaining the asset's currency and security. (Refer also to *ISO/IEC 27002:2005* [3], Clause 7.1.)

4.2 Health information classification (C.2)

Control Objective: To ensure that information receives an appropriate level of protection.

NESAF Ref	Control Category	Control	Control Source
C.2.1	Classification guidelines	Information should be classified in terms of its value, legal requirements, sensitivity, and criticality to the organisation. Organisations processing personal health information should uniformly classify such data as confidential.	*AS ISO 27799-2011* [4] Clause 7.4.2.1

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Business Information Technology	All personal health information is confidential and should be treated accordingly. Ultimately, only the patient can determine if the information is no longer to be considered confidential in nature. Subjects of care that may be at elevated risk of unauthorised access (for example health organisation staff, heads of government, and celebrities) may have their records tagged accordingly so that access can be closely monitored. However, their personal health information is not innately more confidential than that of other subjects of care. Whilst each record of data may have a specific classification marking, for example, “protected”, an aggregation of that data in a database usually increases in higher classification (for example, “highly protected”) and therefore appropriate mitigating controls should reflect this. Please refer to the Asset Classification section of the *NESAF v4.0 Business Blueprint* [2] for additional guidance and information.

NESAF Ref	Control Category	Control	Control Source
C.2.2	Information labelling and handling	All health information systems processing personal health information should inform users of the confidentiality of personal health information accessible from the system and should label hardcopy output as confidential when it contains personal health information.	*AS ISO 27799-2011* [4] Clause 7.4.2.2

Control Type		Responsibility Domain	Notes
People Technology	Preventive	Information Technology	Not all health information is confidential and not all health information systems provide users with access to personal health information. Users of health information systems need to know when the data they are accessing contains personal health information.

NESAF Ref	Control Category	Control	Control Source
C.2.3	De-identification of health information output	Health information systems should enable the de-identification of healthcare information output where such data are used for purposes other than the clinical care of patients.	• *RACGP Handbook for the Management of Health Information in Private Medical Practice* [14] • *NHMRC Privacy Guidelines* [15]

Control Type		Responsibility Domain	Notes
Technology	Preventive	Information Technology	The privacy of personal or health information should be maintained when used for purposes other than clinical care, and in line with privacy law requirements, for instance, research or statistical purposes for public health or public safety. De-identification of personal health information is more than simply removing the patient's name. Whenever the information is in the form of individual data sets, there is a risk that the data set could be linked to a particular individual on the basis of details of age, postcode and medical condition. The more information included in the data set, the greater the risk of identification. Even where data is aggregated, care should be taken that the number of people in each "cell" or sub-group is sufficient to ensure that the privacy of the individuals involved is not compromised. If de-identification is not possible, and where it is impracticable to obtain the consent from the individual involved, the *NHMRC Privacy Guidelines* [15] should be used.

5 Human resources security (Control Area D)

5.1 Prior to employment (D.1)

Control Objective: To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.

NESAF Ref	Control Category	Control	Control Source
D.1.1	Roles and responsibilities	Security roles and responsibilities of employees, contractors and third party users should be defined and documented in accordance with the organisation's information security policy.	• *AS ISO 27799-2011* [4] Clause 7.5.1.1 • *ISO/IEC 27002:2005* [3] Clause 8.1.1

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Business	Involvement in processing personal health information, and security roles and responsibilities, should be documented in relevant job descriptions. Position descriptions should include general responsibilities for information security, including, but not limited to, maintaining the confidentiality of health and personal information. Special attention should be placed on the position descriptions of temporary, casual and other short term staff.

NESAF Ref	Control Category	Control	Control Source
D.1.2	Screening	Background verification checks on all candidates for employment, contractors, and third party users should be carried out in accordance with relevant frameworks and best practices, ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks. All organisations whose staff, contractors or volunteers process (or are expected to process) personal health information should, as a minimum, verify the identity, current address and previous employment of such staff, contractors and volunteers at the time of job applications.	• *AS ISO 27799-2011* [4] Clause 7.5.1.2 • *ISO/IEC 27002:2005* [3] Clause 8.1.2

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Business	Criminal history checks should also be undertaken for all employees or third parties requesting access to the organisation's health information, as well as confirmation of professional qualifications.

NESAF Ref	Control Category	Control	Control Source
D.1.3	Terms and conditions of employment	As part of their contractual obligation, employees, contractors and third party users should agree and sign the terms and conditions of their employment contract, which should state their responsibilities for information security, as well as those of the organisation.	• *AS ISO 27799-2011* [4] Clause 7.5.1.3 • *ISO/IEC 27002:2005* [3] Clause 8.1.3

Control Type		Responsibility Domain	Notes
People	Preventive	Business	The terms and conditions should include the consequences if the information security policy is breached, and specify the rights that the employee will have to access health information and information systems.

5.2 During employment (D.2)

Control Objective: To ensure that employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organisational security policy in the course of their normal work, and to reduce the risk of human error.

NESAF Ref	Control Category	Control	Control Source
D.2.1	Management responsibilities	Management should require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organisation.	*AS ISO 27799-2011* [4] Clause 7.5.2.1

Control Type		Responsibility Domain	Notes
People	Preventive	Business	Management should ensure that employees and third parties are: • Properly briefed on their information security roles and responsibilities prior to being granted access to the system. • Provided with guidelines to state security expectations of their role within the organisation. • Motivated to fulfil the security policies of the organisation.

NESAF Ref	Control Category	Control	Control Source
D.2.2	Information security awareness, education and training	All employees of the organisation and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in the organisation's policies and procedures, as relevant for their job function. All organisations processing personal health information should ensure that information security education and training are provided on induction and that regular updates in organisational security policies and procedures are provided to all employees, contractors, researchers, students and volunteers who process personal health information.	• *AS ISO 27799-2011* [4] Clause 7.5.2.2 • *ISO/IEC 27002:2005* [3] Clause 8.2.2

Control Type		Responsibility Domain	Notes
People	Preventive	Business	Management should implement security awareness training programmes for all employees and third parties of the organisation who access health or personal information. Plans to review the effectiveness of the training should be developed and implemented by management.
Process/ Policy		Information Technology	
		Clinical	

NESAF Ref	Control Category	Control	Control Source
D.2.3	Disciplinary process	There should be a formal disciplinary process for employees who have committed a security breach.	*AS ISO 27799-2011* [4] Clause 7.5.2.3

Control Type		Responsibility Domain	Notes
Process/ Policy	Corrective	Business	Management should develop disciplinary processes and ensure that all employees are aware of the consequences for breaching the information security policy. Users should also be aware of legislative penalties and enforcement powers under privacy or other health information legislation.

5.3 Termination or change of employment (D.3)

Control Objective: To ensure that employees, contractors and third party users exit an organisation or change employment in an orderly manner

NESAF Ref	Control Category	Control	Control Source
D.3.1	Termination responsibilities and return of assets	Responsibilities for performing employment termination or change of employment should be clearly defined and assigned.	*AS ISO 27799-2011* [4] Clause 7.5.3.1

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Business	Changes in employment for example, progression through training programmes and other “rotations” where access rights can change fundamentally, should be processed in the same way as for individuals leaving the organisation’s employ. Consider linking the information security termination process with the human resource termination process to minimise delay with the return of assets and disabling employee or third-party credentials.

NESAF Ref	Control Category	Control	Control Source
D.3.2	Removal of access rights	All organisations that process health information should, as soon as possible, terminate the user access privileges with respect to such information for any departing permanent or temporary employee, third-party contractor or volunteer upon termination of employment, contracting or volunteer activities.	*AS ISO 27799-2011* [4] Clause 7.5.3.2

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Business	Terminated employees or third parties should not have access to health or personal information after leaving the health organisation. Transferred or rotated employees or third parties should not have access to health or personal information, beyond that which is required for their current role. Consider linking the information security termination process with the human resource termination process to minimise delay with the return of assets and disabling employee or third party credentials. Access credentials should not be deleted in case of future creation. It is important to not re-issue credentials (for example, user names) of an employee that has been terminated to another employee.

6 Physical and environmental security (Control Area E)

6.1 Secure areas (E.1.)

Control Objective: To prevent unauthorised physical access, damage, and interference to the organisation's premises and information.

NESAF Ref	Control Category	Control	Control Source
E.1.1	Physical security perimeter	Organisations processing personal health information should use security perimeters (for example, walls, card entry gates or manned reception desks) to protect areas that contain information processing facilities supporting such health applications. These should be protected by appropriate entry controls to ensure that only authorised personnel are allowed access.	*AS ISO 27799-2011* [4] Clause 7.6.1.1

Control Type		Responsibility Domain	Notes
Technology	Preventive	Business	In many health organisations it is expected that physical security measures for information should be co-ordinated with physical security and safety measures for subjects of care. Central information and communications facilities within an organisation (information processing facilities such as data centres, computer rooms, networking wiring closets or communications rooms) should have a defined perimeter with entry controls (for example, locks on doors). **Note:** The *Protective Security Policy Framework* [16] contains measures and procedures that agencies and identified entities can use in implementing physical security controls.

NESAF Ref	Control Category	Control	Control Source
E.1.2	Physical entry controls; securing offices, rooms and facilities; protecting against external and environmental threat; working in secure areas	Secure areas should be protected by appropriate entry controls to ensure that only authorised personnel are allowed access. Physical security for offices, rooms, and facilities should be designed and applied. Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and applied. Physical protection and guidelines for working in secure areas should be designed and applied.	*AS ISO 27799-2011* [4] Clause 7.6.1.2

Control Type		Responsibility Domain	Notes
Process/ Policy Technology	Preventive	Business	Organisations should take sensible steps to ensure that the public are only as close to IT equipment (servers, storage device, terminals and displays) as physical constraints and clinical processes demand. When employees or third parties are working in secure areas (computer or communications rooms), access to these rooms should be monitored and auditable. For example, CCTV, log files of electronic access, locked doors, alarm systems.

NESAF Ref	Control Category	Control	Control Source
E.1.3	Public access, delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorised persons may enter the premises should be controlled, and, if possible, isolated from information processing facilities to avoid unauthorised access.	*AS ISO 27799-2011* [4] Clause 7.6.1.3

Control Type		Responsibility Domain	Notes
Technology	Preventive	Business	Public areas where health information is gathered through interview or that contain systems where data is viewed on screen should be subject to additional scrutiny. For example, placing notices in these areas that remind employees to curtail discussion of patient cases in public areas.

6.2 Equipment security (E.2)

Control Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organisation's activities.

NESAF Ref	Control Category	Control	Control Source
E.2.1	Equipment siting and protection	Equipment should be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.	*AS ISO 27799-2011* [4] Clause 7.6.2.1

Control Type		Responsibility Domain	Notes
Technology	Preventive	Business Information Technology Clinical	Organisations should situate any workstations allowing access to personal health information in a way that prevents unintended viewing or access by subjects of care and the public. Organisations should ensure that the siting and protection guidelines for IT equipment minimise exposure to the public. Consider attaching a privacy filter to screens that may be viewable by the public.

NESAF Ref	Control Category	Control	Control Source
E.2.2	Supporting utilities, cabling security and equipment maintenance	Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities. Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage. Equipment should be correctly maintained to ensure its continued availability and integrity.	*AS ISO 27799-2011* [4] Clause 7.6.2.2

Control Type		Responsibility Domain	Notes
Technology	Preventive	Business Information Technology	Organisations processing personal health information should give serious consideration to the shielding of network and other cabling in areas with high emissions from medical devices. Some geographic areas susceptible to power failures or loss should consider the use of generated power as a backup.

NESAF Ref	Control Category	Control	Control Source
E.2.3	Security of equipment off premises	Security should be applied to off-site equipment taking into account the different risks of working outside the organisation's premises. Organisations processing personal health information should ensure that any use, outside its premises, of medical devices that record or report data has been authorised. This should include equipment used by remote workers, even where usage is perpetual (that is, where it forms a core feature of the employee's role, such as for ambulance personnel, therapists, and so on).	• *ISO/IEC 27002:2005* [3] Clause 9.2.5 • *AS ISO 27799-2011* [4] Clause 7.6.2.3

Control Type		Responsibility Domain	Notes
People	Preventive	Business	Health organisations that regularly utilise equipment containing health or personal information off premises should consider developing a Portable Device Policy and procedures to guide employees in the use and security of such equipment. This is especially important with the advent of personal and organisationally-owned handheld and portable devices being used in healthcare.
Process/ Policy		Information Technology	
Technology		Clinical	

NESAF Ref	Control Category	Control	Control Source
E.2.4	Secure disposal or re-use of equipment	All items of equipment containing storage media should be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal. Organisations processing health information applications should securely overwrite or else destroy all media containing health information application software or personal health information when the media are no longer required for use.	• *ISO/IEC 27002:2005* [3] Clause 9.2.6 • *AS ISO 27799-2011* [4] Clause 7.6.2.4

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Business	Only approved, reputable organisations should be used to resell or dispose of any equipment that may contain, or has transmitted health or personal information. Electronic records that are no longer needed should be deleted (unless retention of such records is required by law). However, it is very difficult to reliably remove all traces of electronically stored information. Organisations will need to be aware that deletion may only remove the file reference but leave all the other information intact. An effective means of removing sensitive information from magnetic devices such as hard drives, magnetic tapes is degaussing, a process of decreasing or eliminating magnetic fields rendering information on the device unrecoverable or able to reconstruct the data. There are secure deletion programs available that overwrite a disk drive with random data thereby effectively deleting the previous confidential data. Other methods may include physical destruction, that is, physically breaking the device.
Technology		Information Technology	
		Clinical	

NESAF Ref	Control Category	Control	Control Source
E.2.5	Removal of property	Equipment, information or software should not be taken off-site without prior authorisation. Organisations providing or using equipment, data or software to support healthcare applications containing personal health information should not allow such equipment, data or software to be removed from the site or relocated within it without authorisation by the organisation.	• *ISO/IEC 27002:2005* [3] Clause 9.2.7 • *AS ISO 27799-2011* [4] 7.6.2.5

Control Type		Responsibility Domain	Notes
People	Preventive	Business	Health organisations that regularly utilise equipment containing health or personal information off premises should consider developing a Portable Device Policy and procedures to guide employees in the use and security of such equipment. The policy should detail the authorisation process for device usage and detail which devices may be used.
Process/ Policy		Information Technology	
		Clinical	

7 Communications and operations management (Control Area F)

7.1 Operational procedures and responsibilities (F.1)

Control Objective: To ensure the correct and secure operation of information processing facilities.

NESAF Ref	Control Category	Control	Control Source
F.1.1	Documented operating procedures	Operating procedures (including processing and handling of information, backup, scheduling requirements, handling errors, support contracts, output and media handling instructions, system restart and recovery, management of audit-trail and system log information) should be documented, maintained, and made available to all users who need them.	*ISO/IEC 27002:2005* [3] Clause 10.1.1

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Information Technology	The organisation should have documented and maintained operating procedure manuals. These manuals should specify the instructions for the detailed execution of each job, including scheduling and any interdependencies, special data processing, specific backup requirements, error handling, specialised support team (where available), start-up and stop processes, and handling of log information including audit trails.

NESAF Ref	Control Category	Control	Control Source
F.1.2	Change management	Changes to information processing facilities and systems should be controlled. Organisations processing personal health information should, by means of a formal and structured change control process, control changes to information processing facilities and systems that process personal health information to ensure the appropriate control of host applications and systems and continuity of patient care.	*AS ISO 27799-2011* [4] Clause 7.7.1.2

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Information Technology	Inadequate or inappropriate testing of changes to information processing facilities and systems is a common cause of system or security failures and can have disastrous consequences for patient safety. Organisations should document change management processes that describe how to assess and identify the risks to the operational environment, especially when transferring a system from development to the operational stage. Large organisations commonly use a service management framework such as ITIL. These frameworks describe a robust change management process that can support the effective management of the information processing environment as business needs require.

NESAF Ref	Control Category	Control	Control Source
F.1.3	Segregation of duties	Duties and areas of responsibility should be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets.	*AS ISO 27799-2011* [4] Clause 7.7.1.3

Control Type		Responsibility Domain	Notes
Process	Preventive	Business	Organisations should where possible, segregate areas of responsibility to reduce the possibility of unauthorised access, modification or misuse of personal information. Small organisations may find segregation of duties difficult to achieve, but the principle should be applied as far as is possible and practicable. Whenever it is difficult to segregate duties, other controls including monitoring of activities, audit trails and management supervision should be considered. It is important that security audit remains independent. Although implementing this control area may commonly be realised by using more than one person in a role to ensure that operations can be monitored, the control needed is often finer-grained. For example, it is good practice to prevent database administrators from being able to also administer the system that audits access to the database. A malicious attacker who might gain access to the database would seek to hide their activities by altering log files or access logs; separating these roles (and systems) is prudent and can provide additional detection capabilities in the event of an attack.

NESAF Ref	Control Category	Control	Control Source
F.1.4	Separation of development, test and operational facilities	Development, test, and operational facilities should be separated to reduce the risks of unauthorised access or changes to the operational system. Organisations processing personal health information should separate (physically or virtually) development and testing environments for health information systems processing such information from operational environments hosting those health information systems. Rules for the migration of software from development to operational status should be defined and documented by the organisations hosting the affected applications.	*ISO/IEC 27002:2005* [3]

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Information Technology	No unauthorised users should be able to access systems to implement changes without following the change management processes (see Control F.1.2). Organisations should ensure that there is clear separation between different environments, especially access to real personal health information. Development and test environments should not use real personal health information unless it has been de-identified or obfuscated as the use of production data may have privacy implications. Separating development, test, and operational facilities is therefore desirable to reduce the risk of accidental change or unauthorised access. That is, configurations of systems in production should be defined in such a way as to reduce the risk of granting inappropriate access to software and or personal health information. Be aware that turning on verbose logging in a production environment may disclose personal health information to system administrators. Also be careful of troubleshooting or tracing code or code that may allow “backdoor” or elevated access.

7.2 Third-party service delivery management (F.2)

Control Objective: To implement and maintain the appropriate level of information security and service delivery in line with third-party service delivery agreements.

NESAF Ref	Control Category	Control	Control Source
F.2.1	Service delivery	It should be ensured that the security controls, service definitions and delivery levels included in the third-party service delivery agreements are implemented, operated, and maintained by the third party.	*ISO/IEC 27002:2005* [3] Clause 10.2.1

Control Type		Responsibility Domain	Notes
Process/ Policy	Detective	Business Information Technology	The contract that describes the service delivery by a third party should include the agreed security arrangements, service definitions, and aspects of service management. It should also describe how the third party will maintain sufficient service capability to ensure that agreed service continuity levels are maintained following major service failures or disaster When outsourcing, an organisation should ensure that the security and integrity of personal health information is maintained throughout the transition period and during the outsourcing contract.

NESAF Ref	Control Category	Control	Control Source
F.2.2	Monitoring and review of third party services	The services, reports and records provided by the third party should be regularly monitored and reviewed, and audits should be carried out regularly.	*ISO/IEC 27002:2005* [3] Clause 10.2.2

Control Type		Responsibility Domain	Notes
Process/ Policy	Detective	Business Information Technology	The organisation should assign a designated individual or service management team the responsibility for managing the third party. The third party should assign responsibilities for checking for compliance and enforcing the requirements of the contractual agreements. Resources should be made available to monitor that requirements of the contractual agreement, in particular the information security requirements, are being met. Appropriate action should be taken when deficiencies are identified. The organisation should maintain overall control and visibility into all security aspects for health information processing facilities accessed, processed or managed by a third party. The organisation should ensure they have tools and resources to enable them to maintain control of change management, identification of vulnerabilities, and information security incident reporting/response. When outsourcing, the organisation needs to be aware that the ultimate responsibility for health information processed by an outsourcing party remains with the organisation.

NESAF Ref	Control Category	Control	Control Source
F.2.3	Managing changes to third party services	Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business systems and processes involved as well as the re-assessment of risks.	*ISO/IEC 27002:2005* [3] Clause 10.2.3

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Business Information Technology	Changes to third party services include updating existing services as well as incorporating new functions. Organisations should ensure that the organisation's change management procedures are followed.

7.3 System planning and acceptance (F.3)

Control Objective: To minimise the risk of systems failures.

NESAF Ref	Control Category	Control	Control Source
F.3.1	Capacity management	The use of resources should be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.	*ISO/IEC 27002:2005* [3] Clause 10.3.1

Control Type		Responsibility Domain	Notes
Technology	Preventive Detective	Information Technology	Systems should be monitored to ensure the availability of systems and to plan for system upgrades. Key system resources, especially those with specialist or extended procurement processes, should have regular updates to future projections of requirements, identifying trends in usage.

NESAF Ref	Control Category	Control	Control Source
F.3.2	System acceptance	Acceptance criteria for new information systems, upgrades, and new versions should be established and suitable tests of the system(s) carried out during development and prior to acceptance. Organisations processing personal health information should establish acceptance criteria for planned new information systems, upgrades and new versions. They should carry out suitable tests of the system prior to acceptance.	*AS ISO 27799-2011* [4] Clause 7.7.3.2

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Information Technology	The organisation should have documented acceptance criteria including the formal testing that must be performed as well as formal sign-off processes. The testing should exercise all aspects of the new system or upgrade and include the operation, user acceptance, functional, business continuity and security functions. The extent and rigour of the testing should be performed by different personnel and should reflect the risks identified in the risk assessment associated with the change. Acceptance criteria should also ensure that there are agreed and documented security controls, business continuity plans and operations/user manuals.

7.4 Protection against malicious and mobile code (F.4)

Control Objective: To protect the integrity of software and information.

NESAF Ref	Control Category	Control	Control Source
F.4.1	Controls against malicious code	Detection, prevention and recovery controls to protect against malicious code and appropriate user awareness procedures should be implemented. Organisations processing personal health information should implement appropriate prevention, detection and response controls to protect against malicious software and should implement appropriate user awareness training.	*ISO/IEC 27002:2005* [3] Clause 10.4.1

Control Type		Responsibility Domain	Notes
People	Preventive	Information Technology	Organisations should ensure that they have anti-malware software running on all devices as well as any network boundary; and that processes are in place to ensure that the anti-malware software and signatures are kept up to date, preferably by automated procedures. The anti-malware software should check the computer hard disk on a regular basis (for example, once per week), as well as any removable storage devices (for example, USB drives, optical media). It should also monitor other ingress point such as email and web browsing. Organisations should document clear policies prohibiting the download and/or installation of unauthorised software, and the use of the organisation's computers for accessing internet sites for non-work related activities, as this could expose the computer to malicious code. Users should be trained and made aware of the policies. Organisations should have documented procedures for how to deal with an infected computer, including business continuity plans and how to recover any log files or audit records to determine if there was any compromise.
Process/ Policy	Detective		
Technology	Corrective		

NESAF Ref	Control Category	Control	Control Source
F.4.2	Controls against mobile code	Where the use of mobile code is authorised, the configurations should ensure that the authorised mobile code operates according to a clearly defined security policy, and unauthorised mobile code should be prevented from executing.	*ISO/IEC 27002:2005* [3] Clause 10.4.2

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Information Technology	Mobile code is software code that transfers from one computer to another and then executes automatically: it normally performs a specific function without any user interaction and is often associated with middleware services. For example, scripts, Java applets, ActiveX controls, macros embedded in documents, and applications sent as attachments via emails.

Control Type		Responsibility Domain	Notes
			Organisations should ensure that any legitimate mobile code that is used within their environment is signed by a trusted code-signing certificate. Organisations should then disable the download and execution of all other mobile code, and should enforce a policy on an exception basis.

7.5 Health information backup (F.5)

Control Objective: To maintain the integrity and availability of information and information processing facilities.

NESAF Ref	Control Category	Control	Control Source
F.5.1	Health information backup	Back-up copies of information and software should be taken and tested regularly in accordance with the agreed backup policy. Organisations processing personal health information should backup all personal health information and store it in a physically secure environment to ensure its future availability. To protect its confidentiality, personal health information should be backed up in an encrypted format.	*AS ISO 27799-2011* [4] Clause 7.7.5

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Information Technology	Processes that support the backing up of health information and essential software so that it can be recovered in the event of a disaster or system failure should be documented and tested. These processes should include what items are to be backed up; how often the back-up is run; what media is used and how it is to be rotated; and where the back-ups are to be stored. The health information that is backed up should be encrypted to ensure its confidentiality. The keys used for the back-up should be changed on a regular basis and should be secured at a separate location from the back-up media. The physical and environmental protection features implemented at the storage site should be consistent with those at the main data centre.

7.6 Network security management (F.6)

Control Objective: To ensure the protection of information in networks and the protection of the supporting infrastructure.

NESAF Ref	Control Category	Control	Control Source
F.6.1	Network controls	Networks should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.	*ISO/IEC 27002:2005* [3] Clause 10.6.1

Control Type		Responsibility Domain	Notes
Technology	Preventive	Information Technology	Organisations should document clear procedures and responsibilities on the management of network equipment and services including controls to ensure the confidentiality and integrity of data passing over the network, especially public and wireless networks; appropriate monitoring and logging to enable clear auditing of events on the network; and clearly defined operational responsibilities, especially if part of the network is provided by a third party. Organisations should also have adequate business continuity measures in place in case of any network failure.

NESAF Ref	Control Category	Control	Control Source
F.6.2	Security of network services	Security features, service levels, and management requirements of all network services should be identified and included in any network services agreement, whether these services are provided in-house or outsourced. Organisations processing personal health information should carefully consider what impact the loss of network service availability will have upon clinical practice.	*AS ISO 27799-2011* [4] Clause 7.7.6.2

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Information Technology	Organisations should ensure that they have documented agreed service features including the security features, service levels and management of the network service. The organisation should have the ability to monitor the network service and should have clearly defined escalation paths if issues are identified. The security features that are identified should include controls for accessing the network, maintaining confidentiality and integrity across the network, and monitoring and reporting on network activity. Organisations should also consider the impacts that loss of the network service will have upon clinical practice.

7.7 Media handling (F.7)

Control Objective: To prevent unauthorised disclosure, modification, removal or destruction of assets, and interruption to business activities.

NESAF Ref	Control Category	Control	Control Source
F.7.1	Management of removable computer media	There should be procedures in place for the management of removable media. Organisations should ensure that all personal health information stored on removable media is: • encrypted while its media are in transit; or • protected from theft while its media are in transit.	*AS ISO 27799-2011* [4] Clause 7.7.7.1

Control Type		Responsibility Domain	Notes
People	Preventive	Business	Organisations should have documented processes for the management of media. When media is no longer required it should be destroyed, degaussed or sanitised so that the information is unrecoverable. All media should be used and stored in accordance with the manufacturer's recommendations; and where necessary media should be refreshed if the storage period exceeds the manufacturers' recommendation. Organisations should disable the use of removable media on computers where there is no business reason. Removable media includes tapes, floppy disks, USB and flash drives, removable hard disk drives, and optical disks (CDs and DVDs). Organisations removing media containing sensitive information to an off-site location should protect against accidental loss or theft through the use of approved encryption technology.
Process/ Policy		Information Technology	
		Clinical	

NESAF Ref	Control Category	Control	Control Source
F.7.2	Disposal of media	Media should be disposed of securely and safely when no longer required, using formal procedures. All personal health information should be securely overwritten or else the media destroyed when no longer required for use.	*AS ISO 27799-2011* [4] Clause 7.7.7.2

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Business	Organisations should have a process in place to control the disposal of unwanted or expired media. All media containing health information (including storage media within a computer or medical device) should be disposed of in a manner which maintains the security of the data. There are programs that can be used to securely remove the information from computer media. These should be used on media before it is removed to ensure that the recovery of information is impossible or impractical from the computer device. Organisations should destroy media
Technology		Information Technology	
		Clinical	

Control Type		Responsibility Domain	Notes
			so that it can no longer be used (for example, incinerate, degauss or shred) if it is not possible to sanitise it. Many accredited organisations offer secure destruction services including certificates of destruction. This may be more practical than the health organisation doing the destruction itself. If using a paper shredder, ensure that it is a cross cut device, not a strip shredder. When accumulating media of a less sensitive nature, organisations should consider that the aggregation of the less sensitive information to become more sensitive. Organisations should consider whether the better approach might be to securely dispose of all media. The Media Destruction section of the *Information Security Manual* [12] cites appropriate methods of disposing various forms of media including: • magnetic floppy disks; • magnetic hard disks; and • magnetic tapes.

NESAF Ref	Control Category	Control	Control Source
F.7.3	Information handling procedures	Procedures for the handling and storage of information should be established to protect this information from unauthorised disclosure of misuse. Media containing personal health information should be either physically protected or else have their data encrypted. The status and location of media containing unencrypted personal health information should be monitored.	*ISO/IEC 27002:2005* [3] Clause 10.7.3

Control Type		Responsibility Domain	Notes
People	Preventive	Information Technology	Organisations should document procedures for the storage, handling, processing and communication of information. Where health information is stored electronically (either permanently or temporarily), it should be encrypted or physical protections should be in place to prevent unauthorised access. Removable media should be marked with the classification and type of data, identified with a unique reference, and if appropriate, the recipient's name. Records should be kept of where the media is stored and who/when the media was accessed. Unencrypted health information, including printed copies, should be clearly marked with the authorised recipient's name and date; and be monitored, including a receipt from the recipient acknowledging acceptance of the media. When the media is no longer required or expired it should be securely destroyed, see Control F.7.2.
Process/ Policy Technology	Detective	Clinical	

NESAF Ref	Control Category	Control	Control Source
F.7.4	Security of system documentation	System documentation should be protected against unauthorised access.	*ISO/IEC 27002:2005* [3] Clause 10.7.4

Control Type		Responsibility Domain	Notes
People	Preventive	Information Technology	System documentation may contain a range of sensitive information, for example, descriptions of applications, processes, procedures, data structures, authorisation processes. System documentation should be securely stored and access should be kept to a minimum and authorised by the application owner. System documentation held on a public network, or supplied via a public network, should be appropriately protected from unauthorised access.

7.8 Exchanges of information (F.8)

Control Objective: To maintain the security of information and software exchanged within an organisation and with any external entity.

NESAF Ref	Control Category	Control	Control Source
F.8.1	Health information exchange policies and procedures and exchange agreements	Formal exchange policies, procedures, and controls should be in place to protect the exchange of information through the use of all types of communication facilities. Agreements should be established for the exchange of information and software between the organisation and external parties.	*AS ISO 27799-2011* [4] Clause 7.7.8.1

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Business Information Technology	Organisations should ensure that all information exchanges are done in accordance with agreed policies and are subject to audit controls. The security of information exchanges should be documented in mutually-agreed information exchange agreements. Organisations should ensure that all personnel that have access to sensitive information understand their responsibilities for ensuring the confidentiality and integrity of that data, including: • Not divulging information to unauthorised parties by means of conversation in a public place, or misplacing or misdirecting media such as print outs or email communications. • Opening of unsolicited or spam emails which may contain malicious code. • Using insecure communication methods, such as facsimile, voicemail, instant messaging.

NESAF Ref	Control Category	Control	Control Source
F.8.2	Physical media in transit	Media containing information should be protected against unauthorised access, misuse or corruption during transportation beyond an organisation's physical boundaries.	*ISO/IEC 27002:2005* [3] Clause 10.8.3

Control Type		Responsibility Domain	Notes
People	Preventive	Business Information Technology Clinical	Information could be vulnerable to unauthorised access, misuse, loss or corruption during physical transport. Appropriate security controls need to be implemented to reflect the classification of the data contained in the media. Organisations should create a list of approved and reliable couriers that meet their security requirements. Only approved couriers should be used to transport media that contains sensitive information. Couriers should be identified before the package is handed over and when the package is received. Media should be transported in secure containers that are tamper evident and should protect the media from any damage that might occur during transit, including environmental factors (for example, moisture, heat, sunlight, and electromagnetic fields).

NESAF Ref	Control Category	Control	Control Source
F.8.3	Electronic messaging	Information involved in electronic messaging should be appropriately protected. Organisations transmitting personal health information should take steps to ensure its confidentiality and integrity.	*AS ISO 27799-2011* [4] Clause 7.7.8.3

Control Type		Responsibility Domain	Notes
People	Preventive	Information Technology	Electronic messaging has different risks to paper-based messaging because of the ease and speed of dissemination. When messages are sent electronically (for example, email, file transfers/file sharing services), organisations should ensure that there are sufficient systems and user education to prevent any sensitive information from being disclosed to an unauthorised party. This should include ensuring that only authorised users can send sensitive information by approved services; and also putting in place systems and processes to ensure correct addressing. Any unapproved messaging services should be disabled, either at the computer or at the network level. Steps should be in place to ensure the confidentiality and integrity of the information within the message. Organisations should also consider whether there is any requirement for authentication of the sender, by using a digital signature for example. Further detail can be found in the Secure Messaging Component section of the *NESAF v4.0 Implementer Blueprint* [5].
Technology		Clinical	

NESAF Ref	Control Category	Control	Control Source
F.8.4	Health information systems	Policies and procedures should be developed and implemented to protect information associated with the interconnection of business information systems.	*ISO/IEC 27002:2005* [3] Clause 10.8.5

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Business	Systems should have the ability to restrict access to some records or information when transferring information to another system. All interconnected systems should maintain the same level of protection of the information that has been ascertained in the risk assessment. Organisations should consider whether different levels of access to information are required for different categories of users (for example, consumer, administrative staff, nurse, health practitioner) and also different types of employees (for example, employee, temporary employee, contractor, or vendor). Organisations should help users to identify the type of an employee within a directory so that users can verify whether a potential recipient contravenes policy.

7.9 Electronic health information services (F.9)

Control Objective: To ensure the security of electronic commerce services, and their secure use.

NESAF Ref	Control Category	Control	Control Source
F.9.1	Electronic commerce and online transactions	Information involved in electronic commerce passing over public networks should be protected from fraudulent activity, contract dispute, and unauthorised disclosure and modification. Information involved in on-line transactions should be protected to prevent incomplete transmission, misrouting, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.	*AS ISO 27799-2011* [4] Clause 7.7.9.1

Control Type		Responsibility Domain	Notes
Technology	Preventive	Information Technology	Organisations should implement their electronic commerce systems so as not to divulge health information unless it is determined to be necessary. If health information is divulged, then the systems should implement controls to maintain the confidentiality and integrity of the health information. Systems that this may affect include billing, medical claims, invoicing and requisitions. Consideration should also be given as to whether there is a requirement that the originator and/or recipient of the transaction is authenticated, and how authorisations are checked. All electronic commerce systems should have logging that provides an auditable trail of the transactions.

NESAF Ref	Control Category	Control	Control Source
F.9.2	Publicly available health information	Publicly available health information (as distinct from personal health information) should be archived. The integrity of publicly available health information should be protected to prevent unauthorised modification. The source (authorship) of publicly available health information should be stated and its integrity should be protected.	*ISO/IEC 27002:2005* [3] Clause 10.9.3

Control Type		Responsibility Domain	Notes
People	Preventive	Business	Organisations should have formal approval processes before information can be published publicly. There should also be processes that review the publication to ensure that it does not divulge protected information and that it is accurate. Once published processes should ensure the integrity of the publication and identify the author(s). Any sensitive health information must be de-identified within the publication, unless consent to publish publicly has been obtained from the individual involved. See "Information asset management components" in the *NESAF v4.0 Implementer Blueprint* [5] for further information.

7.10 Monitoring (F.10)

Control Objective: To detect unauthorised information processing activities.

NESAF Ref	Control Category	Control	Control Source
F.10.1	Audit logging	Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.	*AS ISO 27799-2011* [4] Clause 7.7.10.2

Control Type		Responsibility Domain	Notes
Process/ Policy Technology	Detective	Information Technology	An audit log should uniquely identify the user, date, time and details of the event. Events that should be recorded in an audit log include successful and unsuccessful access attempts, changes to system configurations, use of privileges, activation of alarms or alerts (for example, anti-virus, intrusion detection systems), and the access, creation, updating or archiving of personal health information. When the audit log event is related to the access, creation, updating or archiving of a personal health record, the log should also uniquely identify the patient, and if appropriate, a record of the former information. Audit logs may contain personal information and should therefore be protected from unauthorised access. It is also important that the integrity of the audit log should be maintained.

NESAF Ref	Control Category	Control	Control Source
F.10.2	Audit review	System audit capabilities should be enabled to fulfil patient needs in determining who has accessed or modified their records.	NESAF

Control Type		Responsibility Domain	Notes
Process/ Policy Technology	Preventive	Business	Systems should be able to provide an easy to understand report containing the required information to identify when and by whom a healthcare record was accessed. In the context of PCEHR, the *PCEHR Rules 2012* [17] establishes access controls that allow consumers to control which healthcare provider has access to their PCEHR record via an access list. The access list allows consumers to personally control their eHealth record. The PCEHR system allows consumers to track and monitor activities on their eHealth record through audit logs. The audit log contains details of who has edited or viewed their record. The PCEHR system has notifications sent to the consumer via email or SMS for certain activities on their eHealth record. For non-PCEHR systems or local clinical records, there is no requirement under *Privacy Act 1988 (Cth)* [13] that obliges an organisation to keep a record showing when and by whom personal information or health information was accessed.
	Detective	Information Technology	
		Clinical	

NESAF Ref	Control Category	Control	Control Source
F.10.3	Monitoring system use	Procedures for monitoring use of information processing facilities should be established and the results of the monitoring activities reviewed regularly. An audit logging facility should be operational at all times while the health information system being audited is available for use.	*AS ISO 27799-2011* [4] Clause 7.7.10.3

Control Type		Responsibility Domain	Notes
Process/ Policy	Detective	Business	Monitoring systems should include details of information systems, such as when the system was started and stopped, use of privileged system accounts, configuration changes, operating system and application alerts, access to system files, installation (or removal) of software, I/O device attachment/removal, access violations and alerts from network gateways, firewalls, intrusion detection systems and other security systems. The organisation should have documented processes for how often the monitoring log files are reviewed, which should be related to the risks identified in the information system. Health information systems should be able to present monitoring log information so that the following can be identified: • All users who have accessed or modified a particular patient's health record(s). • All subjects of care whose records have been accessed by a particular user.
Technology		Information Technology	

NESAF Ref	Control Category	Control	Control Source
F.10.4	Protection of log information	Audit records should be secure and tamper-proof. Access to system audit tools and audit trails should be safeguarded to prevent misuse or compromise.	*AS ISO 27799-2011* [4] Clause 7.7.10.4

Control Type		Responsibility Domain	Notes
Technology	Preventive	Information Technology	Audit logs should be tamper evident, to ensure that log entries cannot be added or deleted or modified. The logs should also be backed up. Systems should also monitor the space available on storage media for the audit log and manage the storage capacity for the audit log file(s). Audit records related to personal health records could be used for evidentiary purposes. Therefore, such logs should be recorded so as to provide integrity of the log and all of the required data. These logs should also be archived. **Useful reference:** *ISO 27789:2013* [18]: Audit Trails for electronic health records.

NESAF Ref	Control Category	Control	Control Source
F.10.5	Administrator and operator logs	System administrator and system operator activities should be logged.	*ISO/IEC 27002:2005* [3] Clause 10.10.4

Control Type		Responsibility Domain	Notes
Technology	Detective	Information Technology	These logs should contain the user account, time of the event, information about the event and which processes were involved. The logs should be tamper evident and should be monitored by a party outside of the normal operations team (for example, IT security team or internal audit). System logs can monitored automatically for certain known events and alerts raised to specific teams and individuals; larger organisations should consider implementing such a system.

NESAF Ref	Control Category	Control	Control Source
F.10.6	Fault logging	Faults should be logged, analysed and appropriate action taken.	*ISO/IEC 27002:2005* [3] Clause 10.10.5

Control Type		Responsibility Domain	Notes
Technology	Detective Corrective	Information Technology	Faults detected by system programs or reported by users related to information systems should be logged. The organisation should have processes that identify how the fault is managed, including how the fault was corrected to ensure that no controls have been compromised; and what state the reported fault is in (for example, open, resolved, awaiting vendor patch).

NESAF Ref	Control Category	Control	Control Source
F.10.7	Clock synchronisation	Health information systems supporting time-critical shared care activities should provide time synchronisation services to support tracing and reconstitution of activity timelines where required.	*AS ISO 27799-2011* [4] Clause 7.7.10.7

Control Type		Responsibility Domain	Notes
Technology	Detective	Information Technology	Where an information system utilises a real-time clock, this clock should be synchronised to a recognised time source and set to an agreed time standard, Coordinated Universal Time (UTC) is recommended. See the Time Management section of the *NESAF v4.0 Implementer Blueprint* [5] for further details. Time is a key part in the audit records system, which for personal health records access could be used for evidential purposes. Therefore, systems should ensure that the clocks utilised by such systems are synchronised regularly.

8 Access control (Control Area G)

8.1 Requirements for access control in health (G.1)

Control Objective: To control access to information.

NESAF Ref	Control Category	Control	Control Source
G.1.1	General	Organisations processing personal health information should control access to that information. In general, users of health information systems should only access personal health information when a healthcare relationship exists between the users and the data subject; when the user is carrying out an activity on behalf of the data subject; and when there is a need for specific data to support this activity.	*ISO/IEC 27002:2005* [3] Clause 11.1.1

Control Type		Responsibility Domain	Notes
People	Preventive	Business	Access control rules for healthcare practitioners accessing health information systems should be identified to mitigate the risks identified to the health information. These access control rules should consider both the logical and physical controls (see Section 6 Physical and environmental security (Control Area E)). For further information refer to the Access Components section of the *NESAF v4.0 Implementer Blueprint* [5].
Technology		Information Technology	
		Clinical	

NESAF Ref	Control Category	Control	Control Source
G.1.2	Access control policy	Organisations processing personal health information should have an access control policy governing access to this data. The organisation's policy on access control should be established on the basis of predefined roles with associated authorities which are consistent with, but limited to, the needs of that role. The access control policy, as a component of the information security policy framework described in Section 2.1 Information security policy (Control Area A), should reflect professional, ethical, legal and subject-of-care-related requirements and should take account of the tasks performed by health professionals and the task's workflow.	*AS ISO 27799-2011* [4] Clause 7.8.1.2

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Business	Organisations should have documented policies that include the requirements for registration of new users, the assigning (and removal) of authorisations, and roles within the organisation. Organisations should have segregation of the roles that perform the registration of users and assign the authorisations. Access control rules should identify rules that must always

Control Type		Responsibility Domain	Notes
			be enforced and guidelines that are optional. The policy should identify the rules that govern the monitoring of access control rule enforcement.

8.2 User access management (G.2)

Control Objective: To ensure authorised user access and to prevent unauthorised access to information systems.

NESAF Ref	Control Category	Control	Control Source
G.2.1	User registration	Access to health information systems that process personal health information should be subject to a formal user registration process. User registration procedures should ensure that the level of authentication required of a claimed user identity is consistent with the levels of access that will become available to the user. User registration details should be periodically reviewed to ensure that they are complete, accurate and that access is still required.	*AS ISO 27799-2011* [4] Clause 7.8.2.1

Control Type		Responsibility Domain	Notes
People	Preventive	Information Technology	All healthcare professionals who require access to healthcare information about patients must be uniquely identifiable either by an HPI-I or the relevant HPI-O and local identifier. The local registration process should issue a user with a unique user ID after they have satisfied an evidence of identity check. The registration process should also assign the user ID authorisations to access information and perform functions within applications and services. The registration process should also ensure that the user is aware of any specific organisational access policies, and should include a record of the user's acceptance of such policies, possibly by recording a signed statement. It should also maintain formal records of approved users, and include processes to revoke registration, when a user leaves the organisation, for example. Organisations should consider grouping users into access roles and assigning authorisations to the roles, as opposed to the individual user.
Technology		Clinical	

NESAF Ref	Control Category	Control	Control Source
G.2.2	Patient Registration (anonymous/pseudonymous)	Healthcare information systems should support the ability of patients to receive anonymous or pseudonymous care wherever it is lawful and practicable.	• *ATS ISO 25237-2011* [19] • *National e-Authentication Framework* [20]

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Business	Australian Privacy Principle 2 states that individuals must have the option of not identifying themselves or of using a pseudonym when dealing with an organisation. The relevant exception to this is where it is impracticable to deal with individuals who have not identified themselves (APP 2.2(b)).[3] Refer to the "Pseudonymisation" section of the *NESAF v4.0 Implementer Blueprint* [5]. **Useful reference:** *ATS ISO 25237-2011* [19] *Pseudonymisation*.
Technology	Detective	Information Technology	
	Corrective	Clinical	

NESAF Ref	Control Category	Control	Control Source
G.2.3	Privilege management	The allocation and use of privileges should be restricted and controlled. Several access control strategies can help significantly to ensure the confidentiality and integrity of personal health information: • Role-based access control, which relies upon the professional credentials and job titles of users established during registration to restrict users' access privileges to just those required to fulfil one or more well-defined roles. • Workgroup-based access control, which relies upon the assignment of users to workgroups (such as clinical teams) to determine which records they can access. • Discretionary access control, which enables users of health information systems who have a legitimate relationship to a patient's personal health information (for example, a family physician) to grant access to other users who have no previously established relationship to that patient's personal health information (for example, a specialist).	*AS ISO 27799-2011* [4] Clause 7.8.2.2

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Information Technology	Health information systems should have the allocation of privileges controlled through a formal authorisation process, including the access privileges associated with each component of the system (operating system, database, application); privileges should only be granted when needed; and use of privileges should be monitored and recorded. Where possible systems should utilise routines and programs that do not require the use of privileges. Inappropriate use of system privileges can assist in the breach of system security controls and therefore should be actively discouraged.
Technology			

[3] *Australian Privacy Principles* [21]

NESAF Ref	Control Category	Control	Control Source
G.2.4	User password management	The allocation of passwords should be controlled through a formal management process.	*AS ISO 27799-2011* [4] Clause 7.8.2.3

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Business Information Technology	When users are first registered they should be given in a secure manner a temporary password that is unique to them. The user should be forced to change the temporary password at first use. If a user is to be issued with another temporary password, (for example, when they forget their password), then the user's identity should be validated prior to the issuance of the new password. Authentication credentials such as user names and passwords should never be stored on a computer system in clear text or in an unprotected form (that is, it should be hashed using a strong hashing algorithm and uniquely salted). Time pressures in health delivery situations can make effective use of passwords difficult to employ. Many health organisations have considered the adoption of alternative authentication technologies to address this problem.

NESAF Ref	Control Category	Control	Control Source
G.2.5	Review of user access rights	Management should review users' access rights at regular intervals using a formal process. Special consideration needs to be given to users who will reasonably be expected to provide emergency care, as they may need access to personal health information in emergency situations where a patient may be unable to communicate consent.	*AS ISO 27799-2011* [4] Clause 7.8.2.4

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Business	User access right should be reviewed at frequent periods, (for example, yearly), and after any major change such as change of role or termination of employment. A user's access rights should be reviewed and re-allocated if the user changes roles within the same organisation. Authorisations for higher privileged access should be reviewed more often, for example, monthly, and allocations should be checked to ensure that unauthorised privilege rights have not been obtained. In healthcare systems it is necessary to ensure that an override is incorporated so as to enable emergency access to healthcare information when consent cannot be obtained in a timely manner. See the Consent Management Component section of the *NESAF v4.0 Implementer Blueprint* [5] for further details.

8.3 User responsibilities (G.3)

Control Objective: To prevent unauthorised user access, and compromise or theft of information and information processing facilities.

NESAF Ref	Control Category	Control	Control Source
G.3.1	Password use	Users should be required to follow good security practices in the selection and use of passwords.	*ISO/IEC 27002:2005* [3] Clause 11.3.1

Control Type		Responsibility Domain	Notes
People	Preventive	Business Information Technology Clinical	All users should be advised to keep their passwords secret and not keep a record. The organisation should have a policy that identifies how often a password should be changed and the complexity of the password. Care should be taken to ensure that the policy does not place undue burden upon the user which may cause them to record their passwords. Password rules should encourage longer passwords, which utilise special characters and numbers, and cannot be recycled. Default administrator and user accounts with passwords should never be used and should be changed to a strong complex password as soon after implementation as possible. The selection of a password should be complex enough to mitigate against brute force attacks. As computing processing technologies evolve, simple passwords are susceptible for brute attacks in a short period of time; a better alternative is to use longer passphrases that incorporate both numerical and alphabetical characters, which will decrease the risk of this vulnerability being exploited.

NESAF Ref	Control Category	Control	Control Source
G.3.2	Unattended user equipment	Users should ensure that unattended equipment has appropriate protection.	*ISO/IEC 27002:2005* [3] Clause 11.3.2

Control Type		Responsibility Domain	Notes
People	Preventive	Business Information Technology Clinical	Users should be made aware that computer equipment should not be left unattended with an active user session still logged in. Users should be encouraged to log off the computer system or utilise an appropriate inactivity timeout locking mechanism (for example, screen lock). Screen locks should enable an override by another user in the event that the computer is required by another user.

NESAF Ref	Control Category	Control	Control Source
G.3.3	Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted.	*ISO/IEC 27002:2005* [3] Clause 11.3.3

Control Type		Responsibility Domain	Notes
People	Preventive	Business	Healthcare practitioners should ensure that no healthcare information is left unattended, either in printed form or electronic form. All printed media should be securely destroyed or locked away. All electronic storage media should be secured when not being used, and healthcare information should be removed securely from the media as soon as it is no longer required. Computer screens should be angled so that they are not visible from public areas; privacy guards should be used to reduce the ability for unauthorised personnel view the screen.

8.4 Network access control and operation system access control (G.4)

Control Objective: To prevent unauthorised access to networked services.

NESAF Ref	Control Category	Control	Control Source
G.4.1	Policy on use of network services	Users should only be provided with access to the services that they have been specifically authorised to use.	*ISO/IEC 27002:2005* [3] Clause 11.4.1

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Business	An organisation should have a policy concerning the use of networks and network services. This policy should identify: • The networks and network services which are allowed to be accessed. • Authentication and authorisation procedures for determining who is allowed to access networks and networked services. • Management controls and procedures to protect access to network connections and network services. • Methods to access the network (for example, virtual private network). This control is particularly important for network connections to applications or services that process health information and to users accessing from high-risk locations, for example, public internet, which is outside the organisation's security management and control.
Technology		Information Technology	

NESAF Ref	Control Category	Control	Control Source
G.4.2	User authentication for external connections	Appropriate authentication methods should be used to control access by remote users.	*ISO/IEC 27002:2005* [3] Clause 11.4.2

Control Type		Responsibility Domain	Notes
Technology	Preventive	Information Technology	Remote users should be authenticated to a level commensurate to the risks identified. Please refer to the Remote Access Component section of *NESAF v4.0 Implementer Blueprint* [5] for further details. The connection should use a virtual private network (VPN) or dedicated private lines to provide assurance of the source of connections. If there are a number of devices at the remote site, for example, small satellite office, then the connection should utilise a VPN between the networks, and each user should be treated as if they were on the internal network.

NESAF Ref	Control Category	Control	Control Source
G.4.3	Equipment identification in networks	Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment.	*ISO/IEC 27002:2005* [3] Clause 11.4.3

Control Type		Responsibility Domain	Notes
Technology	Detective	Information Technology	Authentication of the end-point device should be used if only permitted devices are allowed to connect to the network. The device should be issued with a credential that is unique to it. Once the device is successfully authenticated and connected to the network, the user should be authenticated and authorised access to the application or service. See the Device Security Components section of *NESAF v4.0 Implementer Blueprint* [5] for further details.

NESAF Ref	Control Category	Control	Control Source
G.4.4	Remote diagnostic and configuration port protection	Physical and logical access to diagnostic and configuration ports should be controlled.	*ISO/IEC 27002:2005* [3] Clause 11.4.4

Control Type		Responsibility Domain	Notes
Technology	Preventive	Information Technology	Diagnostic and configuration ports should only be available to authorised users and by approval from the manager of the computer service. Ports, services, and similar facilities installed on a computer or network device, which are not

Control Type		Responsibility Domain	Notes
			specifically required for business functionality, should be disabled or removed. Many computer systems, network systems, and communication systems are installed with a remote diagnostic or configuration facility for use by maintenance engineers. If unprotected, these diagnostic ports could provide a means of unauthorised access.

NESAF Ref	Control Category	Control	Control Source
G.4.5	Segregation in networks	Groups of information services, users and information systems should be segregated on networks.	*ISO/IEC 27002:2005* [3] Clause 11.4.5

Control Type		Responsibility Domain	Notes
Technology	Preventive	Information Technology	Networks should be segregated into domains based on the access control policy and access requirements, and should also take into account the relative cost and performance impact of incorporating additional network routing or gateway technology. In addition, segregation of networks should be based on the value and classification of information stored or processed in the network, levels of trust, or lines of business, in order to reduce the total impact of a service disruption. Networks processing health information should be segregated from those networks used for operational purposes (for example, back-up). Consideration should be given to the segregation of wireless networks from internal and private networks. As the perimeters of wireless networks are not well defined, a risk assessment should be carried out in such cases to identify controls (for example, strong authentication, cryptographic methods, and frequency selection) to maintain network segregation.

NESAF Ref	Control Category	Control	Control Source
G.4.6	Network connection control	For shared networks, especially those extending across the organisation's boundaries, the capability of users to connect to the network should be restricted, in line with the access control policy and requirements of the business applications.	*ISO/IEC 27002:2005* [3] Clause 11.4.6

Control Type		Responsibility Domain	Notes
Technology	Preventive	Information Technology	The organisation's access control policy should identify what services should be available to users on a network, and from where the user can access the service. Any unnecessary or unauthorised services should be

Control Type		Responsibility Domain	Notes
			blocked at the network gateway, for example, file transfer services, by closing the network port.

NESAF Ref	Control Category	Control	Control Source
G.4.7	Network routing control	Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.	*ISO/IEC 27002:2005* [3] Clause 11.4.7

Control Type		Responsibility Domain	Notes
Technology	Preventive	Information Technology	The organisation's access control policy should identify networks that can be connected to particular applications and which functions on that application can utilise or connect to that network. For example, if a segregated back-up network is identified, then no users should be connecting to the application from that network.

NESAF Ref	Control Category	Control	Control Source
G.4.8	Secure log-on procedures	Access to operating systems should be controlled by a secure log-on procedure.	*ISO/IEC 27002:2005* [3] Clause 11.5.1

Control Type		Responsibility Domain	Notes
Process/ Policy Technology	Preventive	Information Technology	The procedure for logging into a system should be designed to limit unauthorised access. The log-on procedure should therefore disclose the minimum of information about the system, in order to avoid providing an unauthorised user with any assistance. A log-on procedure should not display system or application identifiers until the log-on process has been successfully completed and display a general notice warning that the computer should only be accessed by authorised users. The log-on procedure should not provide any messages that might aid an unauthorised user and should only validate the log-on information upon completion of all input data. If an error condition arises, the system should not indicate which part of the data is correct or incorrect. The log-on procedure should limit the number of unsuccessful log-on attempts allowed and should record unsuccessful and successful attempts. Consideration should be given to enforcing a time delay before further log-on attempts are allowed or rejecting any further attempts without specific authorisation. Consideration should be given regarding the display of the following information on completion of a successful log-on:

Control Type		Responsibility Domain	Notes
			• Date and time of the previous successful log-on. • Details of any unsuccessful log-on attempts since the last successful log-on.

NESAF Ref	Control Category	Control	Control Source
G.4.9	User identification and authentication	All users should have a unique identifier for their personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user.	*ISO/IEC 27002:2005* [3] Clause 11.5.2

Control Type		Responsibility Domain	Notes
People Technology	Preventive	Business Information Technology Clinical	All users that need to access an information system should have their own unique user ID, including technical support teams, operators, system administrators and application users. The user ID should be able to assist with tracing the activities to an individual. Users should not log on to systems using privileged accounts, and should use their own user ID and temporarily uplift their session to the privileged account. Users accessing health information should be uniquely identified by a user ID. In exceptional circumstances where there is a clear business benefit, the use of a shared user ID for a small, defined group of users, can be used. This should be documented and the members of the group should be reviewed, and if necessary, the password should be changed to ensure that the shared user ID is not compromised. Additional controls to maintain accountability to an individual may be required. However, this is not appropriate for an organisation's access to the PCEHR system, where an organisation must be able to uniquely identify the user of the system. Generic or anonymous access should only be used where the functions being used do not need to be traced (for example, read-only access to public health information). If privileged user IDs are to be used then they should only be issued to a known individual one user at a time, and a record should be kept of the time and date when the individual used the privileged user ID. The password should be changed after each use so that the record is an accurate copy of when the specific individual used the privileged user ID.

NESAF Ref	Control Category	Control	Control Source
G.4.10	Password management system	Systems for managing passwords should be interactive and should ensure quality passwords.	*ISO/IEC 27002:2005* [3] Clause 11.5.3

Control Type		Responsibility Domain	Notes
Technology	Preventive	Information Technology	A password management system should: • Enforce the use of individual user IDs and passwords to maintain accountability. • Allow users to select and change their own passwords and include a confirmation procedure to allow for input errors. • Enforce a choice of quality passwords (see G.3.1). • Enforce password changes (see G.3.1). • Force users to change temporary passwords at the first log-on (see G.2.4). • Maintain a record of previous user passwords and prevent re-use. • Not display passwords on the screen when being entered. • Store password files separately from application system data. • Store and transmit passwords in protected (for example, encrypted or hashed) form.

NESAF Ref	Control Category	Control	Control Source
G.4.11	Use of system utilities	The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.	*ISO/IEC 27002:2005* [3] Clause 11.5.4

Control Type		Responsibility Domain	Notes
Technology	Preventive	Information Technology	System utilities should be limited to the minimum practical number of trusted authorised users. All system utility use should be monitored and recorded, and should require authentication of the user. Organisations should document the policy and procedures for authorising ad hoc use of system utilities. If ad hoc use of a system utility is required, then it should be authorised by a responsible authority and the authorisation should be recorded. The user should only have access to the utility for the duration that has been authorised. System utilities should be segregated from applications software and where segregation of duties is required, they should not be available to application users. All unnecessary software utilities should be removed or disabled.

NESAF Ref	Control Category	Control	Control Source
G.4.12	Session time-out	Inactive sessions should shut down after a defined period of inactivity.	*ISO/IEC 27002:2005* [3] Clause 11.5.5

Control Type		Responsibility Domain	Notes
Technology	Preventive	Information Technology	A time-out facility that clears the screen, and possibly closes the application after a defined period of time should be implemented on computers that are in insecure environments and have access to health information. Consideration should be given to the type of use and environment that the computer is in, for example this control may be less appropriate in the emergency department.

NESAF Ref	Control Category	Control	Control Source
G.4.13	Limitation of connection time	Restrictions on connection times should be used to provide additional security for high-risk applications.	*ISO/IEC 27002:2005* [3] Clause 11.5.6

Control Type		Responsibility Domain	Notes
Technology	Preventive	Information Technology	Connection time controls should be considered for information systems that access health information, especially if access is from a remote connection. The types of restrictions that should be considered are: • Using predetermined time slots, for example, for batch file transmissions, or regular interactive sessions of short duration. • Restricting connection times to normal office hours if there is no requirement for overtime or extended-hours operation. • Considering re-authentication at timed intervals.

8.5 Application and information access control (G.5)

Control Objective: To prevent unauthorised access to information held in application systems.

NESAF Ref	Control Category	Control	Control Source
G.5.1	Information access restriction	Health information systems processing personal health information should authenticate users and should do so by means of authentication involving at least two factors.	*AS ISO 27799-2011* [4] Clause 7.8.5.1

Control Type		Responsibility Domain	Notes
People	Preventive	Business	Restrictions to health information should be based upon the role the individual plays within the information system and the consent settings that have been set by the health record owner. Applications should only output health information that is relevant and authorised for the user. Access restrictions
Process/ Policy	Detective	Information Technology	
Technology	Corrective	Clinical	

Control Type		Responsibility Domain	Notes
			may also differ depending upon from where (and even what device) the user is accessing the application from.

NESAF Ref	Control Category	Control	Control Source
G.5.2	Sensitive system isolation	Sensitive systems should have a dedicated (isolated) computing environment.	*ISO/IEC 27002:2005* [3] Clause 11.6.2

Control Type		Responsibility Domain	Notes
Technology	Preventive	Information Technology	If an information system manages sensitive health information, then it may be necessary to isolate it from other information systems at the discretion of the system owner after a risk analysis. Additional controls should be put into place to control access and monitor activity.

8.6 Mobile computing and teleworking (G.6)

Control Objective: To ensure information security when using mobile computing and teleworking facilities.

NESAF Ref	Control Category	Control	Control Source
G.6.1	Mobile computing and communications	A formal policy should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing and communication facilities.	*AS ISO 27799-2011* [4] Clause 7.8.6.1

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Business	Organisations should have a documented mobile computing policy that identifies requirements that users of such devices should consider. These additional requirements should include physical security of the mobile device; access controls on the mobile device; health information data protection; and anti-malware protection. The policy should outline when and where mobile devices should be used and should give advice to the user on how to ensure that the health information accessed is not compromised. Further information about implementing this control can be found in the Device Security Components section of *NESAF v4.0 Implementer Blueprint* [5].
Technology		Information Technology	

NESAF Ref	Control Category	Control	Control Source
G.6.2	Teleworking	Policies, operational plans and procedures should be developed and implemented for teleworking activities.	*AS ISO 27799-2011* [4] Clause 7.8.6.2

Control Type		Responsibility Domain	Notes
People	Preventive	Business	Organisations should only authorise teleworking if it is believed that sufficient controls are in place to secure the health information being accessed and that a legitimate business benefit is realised. Teleworking can cross national borders, for example, a health practitioner could be connecting from a hotel in a foreign country, and these legal and ethical considerations need to be taken into account when designing and deploying health information systems.

9 Information systems acquisition, development and maintenance (Control Area H)

9.1 Security requirements of information systems (H.1)

Control Objective: To ensure that security is an integral part of information systems.

NESAF Ref	Control Category	Control	Control Source
H.1.1	Security requirements analysis and specification	Statements of business requirements for new information systems, or enhancements to existing information systems should specify the requirements for security controls.	*ISO/IEC 27002:2005* [3] Clause 12.1.1

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Business	Security requirements should be addressed in the specifications, analysis and/or design phases, and expert advisors should be consulted when implementing new or significant changes to health information systems. Accurate records should be maintained to show traceability from original business requirements to actual configuration and implementation, including appropriate justification and authorisation. System requirements for information security and processes for implementing security should be integrated in the early stages of information system projects. Controls introduced at the design stage are significantly cheaper to implement and maintain than those included during or after implementation.

9.2 Correct processing in applications (H.2)

Control Objective: To prevent errors, loss, unauthorised modification or misuse of information in applications.

NESAF Ref	Control Category	Control	Control Source
H.2.1	Uniquely identifying subjects of care	Health information systems processing personal health information should: • ensure that each patient can be uniquely identified within the system; and • be capable of merging duplicate or multiple records if it is found that multiple records for the same patient have been created unintentionally or during a medical emergency.	*AS ISO 27799-2011* [4] Clause 7.9.2.1

Control Type		Responsibility Domain	Notes
Technology	Preventive Corrective	Information Technology	There may be cases (for example, emergency care) when duplicate records have been created for a patient. It is best for organisations to reconcile (merge) these duplicate patient records as soon as possible. Merging of records must be performed with the greatest of care so should use skilled personnel to do so, and it is preferred if the systems used support tools that facilitate merging with low susceptibility to error.

NESAF Ref	Control Category	Control	Control Source
H.2.2	Input data validation	Data input to applications should be validated to ensure that this data is correct and appropriate.	*ISO/IEC 27002:2005* [3] Clause 12.2.1

Control Type		Responsibility Domain	Notes
People	Detective	Clinical	Software applications used in a health organisation need to be capable of providing automatic validation of input. For example, a date field should be defined to only contain dates, and the format of the date should be defined; a name field should not be capable of having numeric characters. The actual validation required for each health organisation may vary, and should be defined through the analysis phase of an implementation project.

NESAF Ref	Control Category	Control	Control Source
H.2.3	Error correction	Where errors in a healthcare information record are identified, it should be possible to annotate information to indicate the nature of the error. Evidence of the original form of the record should be maintained and the time and date of entries, including those correcting errors, should be recorded.	**NESAF**

Control Type		Responsibility Domain	Notes
People	Corrective	Information Technology	As well as providing an ongoing record of client care, medical records are an important legal document. Consequently, documentation errors should be identified, but information should not be deleted from a healthcare record. The *Australian Privacy Principles* [21] include the following points of relevance to this control: • Australian Privacy Principle 12 requires organisations to give an individual access to their personal information, at the request of that individual. • Moreover, Australian Privacy Principle 13 requires that the organisation must take reasonable steps to correct the personal information to ensure that, having regard
Technology		Clinical	

Control Type		Responsibility Domain	Notes
			to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading, in either of the following circumstances: ○ The organisation is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out-of-date, incomplete or irrelevant or misleading. ○ The individual to whom the personal information relates requests the organisation to correct the information.

NESAF Ref	Control Category	Control	Control Source
H.2.4	Control of internal processing	Validation checks should be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.	*ISO/IEC 27002:2005* [3] Clause 12.2.2

Control Type		Responsibility Domain	Notes
Technology	Detective	Information Technology	The design and implementation of applications should ensure that the risks of processing failures leading to a loss of integrity are minimised. Specific areas to consider include: • The use of add, modify, and delete functions to implement changes to data. • The procedures to prevent programs running in the wrong order or running after failure of prior processing. • The use of appropriate programs to recover from failures to ensure the correct processing of data. • Protection against attacks using buffer overruns/overflows.

NESAF Ref	Control Category	Control	Control Source
H.2.5	Message integrity	Requirements for ensuring authenticity and protecting message integrity in applications should be identified, and appropriate controls identified and implemented.	*ISO/IEC 27002:2005* [3] Clause 12.2.3

Control Type		Responsibility Domain	Notes
Process/ Policy Technology	Preventive	Information Technology	An assessment of security risks should be carried out to determine if message integrity is required and to identify the most appropriate method of implementation. At a minimum, message integrity should be used when transferring health information between organisations or other untrusted entities.

NESAF Ref	Control Category	Control	Control Source
H.2.6	Output data validation	Health information systems processing personal health information should provide personally identifying information to assist health professionals in confirming that the electronic health record retrieved matches the patient under treatment.	*AS ISO 27799-2011* [4] Clause 7.9.2.5

Control Type		Responsibility Domain	Notes
People	Preventive	Information Technology	Before relying on information presented by a health information system, health professionals should be shown sufficient information to ensure that the patient they are treating matches the information displayed. Specific requirements for identifying subjects of care should be based on the assessment of risk. Health information hard copies should make it possible to confirm that the printout is complete by indicating the number of pages expected (for example, “p.3 of 5”).
Technology		Clinical	

NESAF Ref	Control Category	Control	Control Source
H.2.7	Data output for the purposes of non-clinical care	When data is sent, exported or printed from healthcare information systems for purposes other than the clinical care of patients, systems should enable a record to be made of the reason and purpose for which data is being provided.	**NESAF**

Control Type		Responsibility Domain	Notes
Technology	Preventive	Information Technology	An example is the provision of patient histories to a coroner which is required by law. In providing data for non-clinical care purposes, organisations should ensure that they have an appropriate authority for doing so. Healthcare organisations should also consider stipulating the terms and conditions of use, storage and destruction of the data.
	Detective		
	Corrective		

9.3 Cryptographic controls (H.3)

Control Objective: To protect the confidentiality, authenticity or integrity of information by cryptographic means.

NESAF Ref	Control Category	Control	Control Source
H.3.1	Policy on the use of cryptographic controls and key management	A policy on the use of cryptographic controls for protection of information should be developed and implemented. This should include, but not be limited to, guidance on the use of digital certificates in healthcare and the management of cryptographic keys.	• *AS ISO 27799-2011* [4] Clause 7.9.3.1 • *ISO/IEC 27002:2005* [3] Clause 12.3.1

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Information Technology	The policy should include, but not be limited to: • approved cryptographic algorithms; • approved cryptographic protocols; and • key management. For further information, see the Secure Messaging Component of the *NESAF v4.0 Implementer Blueprint* [5].

NESAF Ref	Control Category	Control	Control Source
H.3.2	Key management	Key management should be in place to support the organisation's use of cryptographic techniques.	*ISO/IEC 27002:2005* [3] Clause 12.3.2

Control Type		Responsibility Domain	Notes
Technology	Preventive	Information Technology	Keys to digital certificates should be protected. If the key is compromised, it is possible to obtain access to health information secured by any certificate, moreover, information encrypted by the private key may be rendered unrecoverable. Certificat-issuing authorities or holders of private keys should ensure that keys are protected accordingly. The relevant considerations would include: • Audit logs. • Key management – how keys are stored, revoked, transferred, and installed. • Maintenance. • Objectives of the keys and their use. • System description. • Topology. For further information, see the Secure Messaging Components section of the *NESAF v4.0 Implementer Blueprint* [5].

9.4 Security of system files (H.4)

Control Objective: To ensure the security of system files.

NESAF Ref	Control Category	Control	Control Source
H.4.1	Control of operational software	There should be procedures in place to control the installation of software on operational systems.	*ISO/IEC 27002:2005* [3] Clause 12.4.1

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Information Technology	Procedures should include, but not be limited to: • Testing before implementing into production. • A rollback strategy in case of error in the software release. • Documentation of software versions. • Authorisation to install.

NESAF Ref	Control Category	Control	Control Source
H.4.2	Protection of system test data	Test data should be selected carefully, and protected and controlled. Health or personal information should not be used for testing purposes.	• *AS ISO 27799-2011* [4] Clause 7.9.4.2 • *ISO/IEC 27002:2005* [3] Clause 12.4.2

Control Type		Responsibility Domain	Notes
Technology	Preventive	Information Technology	Identifying information should be de-identified prior to being used for testing purposes. If personal or health information is used for testing purposes, all sensitive details and content should be removed or modified beyond recognition before use. The following guidelines should be applied to protect health or personal information, when used for testing purposes: • The access control procedures that apply to operational health information systems should also apply to test application systems. • There should be a separate authorisation each time that operational information is copied to a test application system. • Operational information should be erased from the test application system immediately after the testing is complete. • The copying and use of operational information should be logged to provide an audit trail.

NESAF Ref	Control Category	Control	Control Source
H.4.3	Access control to program source code	Access to program source code should be restricted.	*ISO/IEC 27002:2005* [3] Clause 12.4.3

Control Type		Responsibility Domain	Notes
Technology	Preventive	Information Technology	To prevent the introduction of unauthorised functionality and to avoid unintentional changes to applications, the source code of an application should be controlled. For program source code, this can be achieved by controlled central storage of such code, preferably in program source libraries on secured storage.

9.5 Security in development and support processes, and technical vulnerability management (H.5)

Control Objective: To maintain the security of application system software and information and to reduce risks resulting from exploitation of published technical vulnerabilities.

NESAF Ref	Control Category	Control	Control Source
H.5.1	Change control procedures	The implementation of changes should be controlled by the use of formal change control procedures.	*ISO/IEC 27002:2005* [3], Clause 12.5.1

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Information Technology	Changes to health information or ICT systems should be managed through formal processes which include an assessment of the impact (positive or negative) that the change may have on the organisation, the responsibilities and method of approval. Without change management, it may be possible for inexperienced employees or third parties to make an unauthorised change to a system that has unforeseen or disastrous impacts.

NESAF Ref	Control Category	Control	Control Source
H.5.2	Technical review of applications after operating system changes	When operating systems are changed, business-critical applications should be reviewed and tested to ensure there has been no adverse impact on organisational operations or security.	*ISO/IEC 27002:2005* [3] Clause 12.5.2

Control Type		Responsibility Domain	Notes
Technology	Preventive	Information Technology	The change management process described previously should also include a post-implementation review of the status of the change prior to confirmation of the change's success. One or several user representatives should be assigned to test the availability and performance of the system. If the change does not pass the technical review, it should be rolled back to the previous state.

NESAF Ref	Control Category	Control	Control Source
H.5.3	Restrictions on changes to software packages	Modifications to software packages should be discouraged, limited to necessary changes, and all changes should be strictly controlled.	*ISO/IEC 27002:2005* [3] Clause 12.5.3

Control Type		Responsibility Domain	Notes
Technology	Preventive Corrective	Information Technology	Except for specifically customisable fields and configuration settings, other modifications to software have the potential to introduce new system vulnerabilities if uncontrolled. If an application does need to be modified then strict change control processes needs to be established, and quality and security testing should be implemented to ensure the same, or higher level of quality as the original software. It is advisable that all original software should be retained in its original version in case of rollback.

NESAF Ref	Control Category	Control	Control Source
H.5.4	Information leakage	Opportunities for information leakage should be prevented.	*ISO/IEC 27002:2005* [3] Clause 12.5.4

Control Type		Responsibility Domain	Notes
Technology	Preventive	Information Technology	The following should be considered to limit the risk of information leakage: • Scanning of outbound media and communications for health information – see also Removable Media (NESAF Ref F.7.1) in Section 7.7. • Making use of reputable systems and software. • Regular monitoring of personnel and system activities, where permitted under existing legislation or regulation. • Monitoring resource usage in computer systems.

NESAF Ref	Control Category	Control	Control Source
H.5.5	Outsourced software development	Outsourced software development should be supervised and monitored by the organisation.	*ISO/IEC 27002:2005* [3] Clause 12.5.5

Control Type		Responsibility Domain	Notes
Technology	Preventive	Business	Where software development is outsourced, the following points should be considered: • Licensing arrangements, code ownership, and intellectual property rights. • Certification of the quality and accuracy of the work carried out. • Escrow arrangements in the event of failure of the third party. • Rights of access for audit of the quality and accuracy of work done. • Contractual requirements for quality and security functionality of code. • Testing before installation to detect malicious and Trojan code, for example, security code reviews by independent third parties.
	Detective	Information Technology	

NESAF Ref	Control Category	Control	Control Source
H.5.6	Control of technical vulnerabilities	Timely information about technical vulnerabilities of information systems being used should be obtained, the organisation's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.	*ISO/IEC 27002:2005* [3] Clause 12.6.1

Control Type		Responsibility Domain	Notes
Technology	Preventive	Information Technology	The management of vulnerabilities in a health organisation's infrastructure is an important part of the overall information security management framework. A health organisation's vulnerability management process should incorporate: • Asset inventory and security baseline – identify the organisation's systems and define a baseline (minimum acceptable standard of security controls) for each group of assets or technology. • Monitor for vulnerability announcements, patch updates and other remediations. This information can be obtained by subscribing to reputable sources such as the Australian Computer Emergency Response Team (AusCERT) or the Common Vulnerabilities and Exposures (CVE)[4]. • Analyse and prioritise the remediations for specific

[4] http://cve.mitre.org/.

Control Type		Responsibility Domain	Notes
			information systems. For instance, an internet-facing system which has been determined to have a critical vulnerability should be prioritised for remediation. • Remediate – apply the patch or other remediation and verify that the vulnerability has been remediated. • Report on the status to information security governors.

10 Information security incident management (Control Area I)

10.1 Reporting information security events and weaknesses (I.1)

Control Objective: To ensure that information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

NESAF Ref	Control Category	Control	Control Source
I.1.1	Reporting information security events and weaknesses	Information security events should be reported through appropriate management channels as quickly as possible. Health organisations should establish security incident management responsibilities and procedures.	• *ISO/IEC 27002:2005* [3] Clause 13.1.1 • *AS ISO 27799-2011* [4] Clause 7.10.1

Control Type		Responsibility Domain	Notes
People	Detective	Business	Organisations should inform the patient whenever their personal information has been unintentionally disclosed. Amongst other areas of interest, Information Security Incident Management procedures should cover: • Planning and preparing for information security incidents. • Detection and reporting of information security events or weaknesses which may become incidents. Consider referring to *ISO/IEC 27035:2011* [22] *Information technology - Security techniques*, and the *OAIC data breach notification guide* [23] for further guidance.
	Corrective	Information Technology	
		Clinical	

10.2 Management of incidents and improvements (I.2)

Control Objective: To ensure a consistent and effective approach is applied to the management of information security incidents.

NESAF Ref	Control Category	Control	Control Source
I.2.1	Responsibilities and procedures	Management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents.	*ISO/IEC 27002:2005* [3] Clause 13.2.1

Control Type		Responsibility Domain	Notes
Process/ Policy	Detective Corrective	Business	Information Security Incident Management procedures should cover: • Planning and preparing for information security incidents. • Detection and reporting of information security events or weaknesses which may become incidents. • Incident response training. • Assessment of the incident and decision making. • Response – both immediate and later responses, which may include forensic analysis. • Lessons learnt. • Reporting and Review. Consider referring to *ISO/IEC 27035:2011* [22] *Information technology - Security techniques* for further guidance.

NESAF Ref	Control Category	Control	Control Source
I.2.2	Learning from incidents	There should be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.	*ISO/IEC 27002:2005* [3] Clause 13.2.2

Control Type		Responsibility Domain	Notes
Process/ Policy	Detective	Information Technology	The analysis of "Lessons Learnt" should include: • An analysis of the underlying (root) cause of the incident. • Any requirements for new or changed information security controls (consider both technical and non-technical – including policy framework changes). • Any required update to the Information Security Risk Register. • Any required changes to the Incident Management procedure including any required tools or capabilities.

NESAF Ref	Control Category	Control	Control Source
I.2.3	Collection of evidence	Where a follow-up action against a person or organisation after an information security incident involves legal action (either civil or criminal), evidence should be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).	• *AS ISO 27799-2011* [4] Clause 7.10.2.3 • *ISO/IEC 27002:2005* [3] Clause 13.2.3

Control Type		Responsibility Domain	Notes
Process/ Policy	Detective	Business Information Technology	Where identified as required for forensic purposes, some further investigation may be required after the incident has been controlled. The analysis should involve the use of IT-based investigative/monitoring techniques and tools, which are accompanied by supporting documented procedures. The aim of the forensic analysis is to review the designated information security event or incident in more depth. External assistance (through certified Forensic Analysts or law enforcement organisations) will usually be required to ensure that any chain of evidence is maintained.

11 Information security aspects of business continuity management (Control Area J)

11.1 Including information security in the business continuity management process (J.1)

Control Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

NESAF Ref	Control Category	Control	Control Source
J.1.1	Including information security in the business continuity management process	A managed process should be developed and maintained for business continuity throughout the organisation that addresses the information security requirements needed for the organisation's business continuity.	*ISO/IEC 27002:2005* [3] Clause 14.1.1

Control Type		Responsibility Domain	Notes
People	Preventive	Business	Business continuity management within health organisations should include health crisis management planning. In an eHealth environment, planning for the continuity of IT services becomes especially important. The organisation should look at any single points of failure of the electronic services and determine how they would conduct healthcare in the event of an IT outage. There are often manual workarounds in place which should be documented and tested regularly.
Process/ Policy		Information Technology	

NESAF Ref	Control Category	Control	Control Source
J.1.2	Business continuity and risk assessment	Events that can cause interruptions to business processes should be identified, along with the probability and impact of such interruptions and their consequences for information security.	*ISO/IEC 27002:2005* [3] Clause 14.1.2

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Information Technology	Risks to business interruptions, specifically through the unavailability information or information systems, should be formally identified and assessed in accordance with the *NESAF v4.0 Business Blueprint* [2]. *ISO 31000:2009* [24] contains further detailed guidance on Risk Management. *AS/NZS 5050:2010* [25] *Managing Disruption Related Risk* may provide further information.

NESAF Ref	Control Category	Control	Control Source
J.1.3	Developing and implementing continuity plans including information security	Plans should be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.	*ISO/IEC 27002:2005* [3] Clause 14.1.3

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Business	The business continuity planning process should include: • Identification and agreement of all responsibilities and business continuity procedures. • Identification of the acceptable loss of information, services or people. • Implementation of the procedures to allow recovery and restoration of healthcare operations and availability of information in required time-scales; particular attention needs to be given to the assessment of internal and external business dependencies and the contracts in place. • Operational procedures to be followed pending completion of recovery and restoration. • Documentation of agreed procedures and processes. • Appropriate education of staff in the agreed procedures and processes, including crisis management. • Testing and updating of the plans.
	Corrective	Information Technology	

NESAF Ref	Control Category	Control	Control Source
J.1.4	Business continuity planning framework	A single framework of business continuity plans should be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.	*ISO/IEC 27002:2005* [3] Clause 14.1.4

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Business	A business continuity framework within a health organisation would usually consist of: • The organisation's Business Continuity Plan (BCP). This should be the main document and include when to activate the plan (disaster declaration) and other governance details. • Larger health organisations may also have specific BCPs for each division or unit, for instance IT Service Continuity Plan; HR Continuity Plan. • Emergency Response Procedures – this is a legislative requirement and includes evacuation and other facility specific information.
		Information Technology	

Control Type		Responsibility Domain	Notes
			• Disaster Recovery Plans – usually IT specific, these are plans and procedures advising how to recover IT services in the event of a disaster.

NESAF Ref	Control Category	Control	Control Source
J.1.5	Testing, maintaining and re-assessing business continuity plans	Business continuity plans should be tested and updated regularly to ensure that they are up-to-date and effective.	*ISO/IEC 27002:2005* [3] Clause 14.1.5

Control Type		Responsibility Domain	Notes
People	Preventive	Business	Health organisations need to make sure that their business continuity plans are tested on a regular basis. The tests should build upon one another, starting from desktop testing (all test personnel sitting at a desk) to modular testing (testing individual components of the plan) to a full rehearsal (testing that the organisation, personnel, equipment, facilities, and processes can cope with interruptions). Results of the testing may result in an update of their business continuity plans.
Process/ Policy		Information Technology	
Technology		Clinical	

12 Compliance (Control Area K)

12.1 General (K.1)

Control Objective: Establish a graduated compliance auditing framework.

NESAF Ref	Control Category	Control	Control Source
K.1.1	General	Health organisations should put a compliance auditing programme in place that addresses the full life cycle of operations, that is, not just of those processes that identify issues, but also of those that review outcomes and that decide on updates to the Information Security Management System (ISMS). Health organisations' audit programmes should be formally structured to cover all elements of this framework, all areas of risk and all implemented controls, within a 12 to 18 month cycle.	*AS ISO 27799-2011* [4] Clause 7.12.1

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Business	In the highly regulated and audited environment of many health organisations, those responsible for the governance of information security should set a goal to establish a multi-tiered compliance framework. At the bottom layer is self-audit by process owners and managers. Thereafter, there should be an independent internal audit followed by external audits by qualified auditors or assessors.

12.2 Compliance with legal requirements (K.2)

Control Objective: To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.

NESAF Ref	Control Category	Control	Control Source
K.2.1	Identification of applicable legislation, intellectual property rights and protection of organisational records	All relevant statutory, regulatory and contractual requirements and the organisation's approach to meet these requirements should be explicitly defined, documented and kept up to date for each information system in the organisation. Appropriate procedures should be implemented to ensure compliance with legislative, regulatory and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products. Important records should be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual and business requirements.	*ISO/IEC 27002:2005* [3] Clauses 15.1.1 to 15.1.3

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Business	As each state and territory may have differing legislative requirements, each healthcare organisation needs to specifically identify legislation or other regulatory or contractual requirements and procedures that support the organisation's compliance to such. Health records should be protected from loss, destruction and falsification. The *NESAF v4.0 Implementer Blueprint* [5] contains specific details regarding the compliance requirements of each security and access component.

NESAF Ref	Control Category	Control	Control Source
K.2.2	Data protection and privacy of personal information	Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses. Organisations processing personal health information should manage consent of subjects of care to the collection, use and disclosure of their personal health information. Consent of subjects of care, where practicable, must be obtained before personal health information is emailed, faxed, or communicated by telephone conversation, or otherwise disclosed to parties external to the healthcare organisation.	• *ISO/IEC 27002:2005* [3] Clause 15.1.4 • *AS ISO 27799-2011* [4] Clause 7.12.2.2

Control Type		Responsibility Domain	Notes
People	Preventive	Business	Relevant privacy legislation (state, territory or federal) should be complied with at all times by health organisations. Refer to the *NESAF v4.0 Implementer Blueprint* [5] for Consent Management Security and Access Component.
Process/ Policy		Information Technology	
Technology		Clinical	

NESAF Ref	Control Category	Control	Control Source
K.2.3	Prevention of misuse of information-processing activities and regulation of cryptographic controls	Users should be deterred from using information processing facilities for unauthorised purposes. Cryptographic controls should be used in compliance with the relevant agreements, laws and regulations.	*ISO/IEC 27002:2005* [3] Clause 15.1.5

Control Type		Responsibility Domain	Notes
People	Preventive	Business	Management should approve the use of information processing facilities. Organisations can implement security policies such as "acceptable use of ICT facilities policy" to deter

Control Type		Responsibility Domain	Notes
			unauthorised use of ICT facilities. If any unauthorised activity is identified by monitoring or other means, this activity should be brought to the attention of the individual manager concerned for consideration of appropriate disciplinary and/or legal action. Consider seeking legal advice prior to implementing monitoring of employee activities, which should take into account the relevant legislation on employee surveillance. At log-on, a warning message should be presented to indicate that the information or information system being accessed is owned by the organisation and that unauthorised access is not permitted.

12.3 Compliance with security policies and standards and technical compliance (K.3)

Control Objective: To ensure compliance of systems with organisational security policies and standards.

NESAF Ref	Control Category	Control	Control Source
K.3.1	Compliance with security policies and standards	Managers should ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.	*ISO/IEC 27002:2005* [3] Clause 15.2.1

Control Type		Responsibility Domain	Notes
People	Preventive	Business Information Technology Clinical	Managers should be responsible for ensuring that the employees and third parties that report to them are compliant with information security policies. This should be both proactive (regular reviews) and reactive (reporting of weaknesses or events when they happen). If any non-compliance is found as a result of a review, managers should: • Determine the causes of the non-compliance. • Evaluate the need for actions to ensure that non-compliance does not recur. • Determine and implement appropriate corrective action. • Review the corrective action taken.

NESAF Ref	Control Category	Control	Control Source
K.3.2	Technical compliance checking	Information systems should be regularly checked for compliance with security implementation standards.	*ISO/IEC 27002:2005* [3] Clause 15.2.2

Control Type		Responsibility Domain	Notes
People	Detective	Information Technology	Employees or third parties responsible for the maintenance and operation of IT systems should ensure that checks are run regularly. Such testing may be performed internally or by external assessors, using automated tools or manually. Where vulnerability scanning or penetration testing techniques are used, the assessor should be qualified, as damage may be caused if not used correctly.

12.4 Information systems audit considerations in a health environment (K.4)

Control Objective: To maximise the effectiveness of and to minimise interference to or from the information systems audit process.

NESAF Ref	Control Category	Control	Control Source
K.4.1	Information systems audit controls	Audit requirements and activities involving checks on operational systems should be carefully planned and agreed, to minimise the risk of disruptions to business processes.	*ISO/IEC 27002:2005* [3] Clause 15.3.1

Control Type		Responsibility Domain	Notes
Process/ Policy	Preventive	Information Technology	When a health organisation's systems are being audited, the following need to be considered to protect health or personal information. • Audit requirements and scope should be agreed with appropriate management. • Checks should be limited to read-only access to software and data. • Access other than read-only should only be allowed for isolated copies of system files, which should be erased when the audit is completed, or given appropriate protection if there is an obligation to keep such files under audit documentation requirements. • Resources for performing the checks should be explicitly identified, made available, documented and authorised. • All access should be monitored and logged to produce a reference trail and the use of time-stamped reference trails should be considered for critical data or systems. • All procedures, requirements, and responsibilities should be documented. • The person(s) carrying out the audit should be independent of the activities audited.

Acronyms

Acronym	Description
AGIMO	Australian Government Information Management Office
AHPRA	Australian Health Practitioners Registration Authority
CCA	Compliance, Conformation and Accreditation (NEHTA programme)
CCOW	Clinical Context Object Workgroup (HL7 standard)
DSML	Directory Services Mark-up Language
GBAC	Governance Based Access Control
GSEF	Gold Standard Enrolment Framework
HPI-I	Healthcare Provider Identifier Individual
HPI-O	Healthcare Provider Identifier Organisation
ICT	Information and Communications Technology
IMAGE	Identity Management for Australian Government Employees
IRAL	Identity Registration Authority Level
ISMF	Information Security Management Forum
ISMS	Information Security Management System
LAN	Line Area Network
MAC	Mandatory Access Control
NASH	National Authentication Service for Health
NeAF	National e-Authentication Framework
NEHTA	National E-Health Transition Authority
NESAF	National E-Health Security and Access Framework
OTP	One time password
PAS	Platform as a service
PHI	Protected Health Information
PKI	Public Key Infrastructure
RACGP	Royal Australian College of General Practitioners
SAML	Security Assertion Markup Language
SEHR	Shared Electronic Health Record
SOE	Standard Operating Environment
SPML	Service Provisioning Markup Language
TLS	Transport Layer Security
VOIP	Voice Over IP
VPN	Virtual Private Network
WAN	Wide Area Network
XACML	XML Access Control Language

Glossary

Term	Definition
Access Control	A means of controlling access by users to computer systems or to data on a computer system.
Asset	Anything that has value to an organisation. *AS ISO 27799-2011* [4]
Authentication	Means that one can verify whether the sender is who they say they are. *RACGP security standards and templates* [11]
Authorised Employee	An authorised employee is an individual that will act on behalf of the healthcare organisation and may be associated with different types of roles within the healthcare organisation, inclusive of healthcare providers and administrative staff who have a legitimate role in accessing systems containing healthcare information.
Availability	Refers to the property of being accessing and usable on demand by an authorised entity. *AS ISO 27799-2011* [4]
Clinical Safety	Clinical safety is concerned with identification and reduction of harm to patients to acceptable levels.
Confidentiality	The property that information is not made available or disclosed to unauthorised individuals, entities or processes.
Control	A means of managing risk, including policies, procedures, guidelines, practices or organisational structures, which can be of administrative, technical, management, or legal nature. Also used as a synonym for safeguard or countermeasure. *ISO/IEC 27002:2005* [3]
De-identified	A record that cannot be linked to an individual.
Denial of service	An attack that results in preventing authorised access and availability of organisational information/services/resources.
Encryption	Data is electronically “scrambled” so that it cannot be read unless the information is decrypted. *RACGP security standards and templates* [11]
Health information system	Repository of information regarding the health of a subject of care in computer-process-able form, stored and transmitted securely, and accessible by multiple authorised users. *AS ISO 27799-2011* [4]
Health professional Healthcare professional	A person who is authorised by a recognised body to be qualified to perform certain health duties. *AS ISO 27799-2011* [4]
Healthcare	Any type of service provided by professionals or paraprofessionals with an impact on health status. *AS ISO 27799-2011* [4]
Healthcare Identifier Service.	The Healthcare Identifier Service assigns a unique national Healthcare Identifier to each healthcare recipient and healthcare provider to establish and maintain accurate records to support the communication and management of health information.
Healthcare organisation	Generic term used to describe many types of organisations that provide healthcare services. *AS ISO 27799-2011* [4]
Healthcare provider	A person who is involved in or associated with healthcare delivery. A synonym for clinician and healthcare professional.
Healthcare Provider Identifier Individual (HPI-I)	A Healthcare Provider Identifier Individual (HPI-I) is a national unique 16-digit identifying number assigned to health practitioners who provide healthcare services to the general public.

Term	Definition
Healthcare Provider Identifier Organisation (HPI-O)	A Healthcare Provider Identifier Organisation (HPI-O) is a national unique 16-digit identifying number assigned to organisations involved in delivering healthcare services.
Information security	Preservation of confidentiality, integrity and availability of information.
Integrity	Refers to the property that data has when it has not been altered or destroyed, or a system has when it can perform its intended function in an unimpaired manner, free from deliberate or accidental unauthorised manipulation of the system. *AS ISO 27799-2011* [4]
Jailbreaking	Process that allows a user to install software not authorised or approved by a mobile device manufacturer.
Malicious code	Programs such as viruses and worms designed to exploit weaknesses in computer software and replicate and/or attach themselves to other software programs on a computer or a network.
Personal health information	Information about an identifiable person which relates to the physical or mental health of the individual or to provision of health services to the individual. *AS ISO 27799-2011* [4]
Personnel	People accessing health data through means owned or provided by the organisation. Includes, staff, contractors, consultants, visiting medical officers and so on.
Privacy	The protection and appropriate handling of information which identifies (or could be used to reasonably ascertain the identity of) an individual.
Provenance	A method to enforce security requirements by means of protecting the traces of historical data or information from its creation and transition to its current state. I can be thought of as an electronic “chain of custody”.
Public Key Infrastructure (PKI)	A set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.
Relying Party	An entity that relies upon an authentication credential
Risk	The probability that a given threat will exploit a given vulnerability. *HB 174-2003* [26]
Risk assessment	The process of identifying risks to a business and determining the probability of occurrence, the resulting impact, and identifying actions that would treat the risk.
Threat	An action or event that may result in a detrimental outcome to a system or information asset. *HB 174-2003* [26]
Trojan	A program that appears legitimate, but performs some illicit activity when it is run.
Vulnerability	A weakness that can be exploited that may cause damage to a system or information assets. *HB 174-2003* [26]

References

1. NEHTA. *National eHealth Security and Access Framework v4.0: Overview*. Sydney: NEHTA; 2014. Available from: http://www.nehta.gov.au/our-work/security.

2. NEHTA. *National eHealth Security and Access Framework v4.0: Business Blueprint*. Sydney: NEHTA; 2014. Available from: http://www.nehta.gov.au/our-work/security.

3. International Organization for Standardization. *ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management*. ISO; 2005. Available from: http://infostore.saiglobal.com/store/.

4. Standards Australia. *AS ISO 27799-2011: Information security management in health using ISO/IEC 27002*. Standards Australia; 2011. Identical to ISO 27799:2008. Available from: http://infostore.saiglobal.com/store/.

5. NEHTA. *National eHealth Security and Access Framework v4.0: Implementer Blueprint*. Sydney: NEHTA; 2014. Available from: http://www.nehta.gov.au/our-work/security.

6. NEHTA. *NESAF v4.0: Factsheet for consumers.* Sydney: NEHTA; 2013 Available from: http://www.nehta.gov.au/our-work/security.

7. NEHTA. *NESAF v4.0: Factsheet for clinicians.* Sydney: NEHTA; 2013 Available from: http://www.nehta.gov.au/our-work/security.

8. NEHTA. *NESAF v4.0: Factsheet for healthcare organisations.* Sydney: NEHTA; 2013 Available from: http://www.nehta.gov.au/our-work/security.

9. NEHTA. *National eHealth Security and Access Framework v4.0: Framework Model and Controls*. Sydney: NEHTA; 2014. Available from: http://www.nehta.gov.au/our-work/security.

10. NEHTA. *National eHealth Security and Access Framework v4.0: Standards Mapping*. Sydney: NEHTA; 2014. Available from: http://www.nehta.gov.au/our-work/security.

11. Royal Australian College of General Practitioners. *Computer and information security standards and templates*. 2013. Available from: http://www.racgp.org.au/your-practice/standards/ciss/.

12. Australian Government. *ISM – Information Security Manual.* [Internet]. [cited 2013 Aug 15]. Available from: http://www.dsd.gov.au/index.htm.

13. Australian Government. *The Privacy Act.* [Internet]. [cited 2014 Jun 02]. Available from: http://www.comlaw.gov.au/Details/C2014C00076.

14. Royal Australian College of General Practitioners. *RACGP Handbook for the Management of Health Information in Private Medical Practice*. RACGP. Login required to download. Available from: http://www.racgp.org.au/your-practice/business/tools/safetyprivacy/privacy/.

15. National Health and Medical Research Council. *Guidelines approved under Section 95A of the Privacy Act 1988*. NHRMC; 2001. ISBN 1864961139. Available from: http://www.nhmrc.gov.au/.

16. Australian Government Attorney-General's Department. *Protective Security Policy Framework.* [Internet]. [cited 2013 Aug 15]. Available from: http://www.protectivesecurity.gov.au/Pages/default.aspx.

17. Australian Government. *PCEHR Rules 2012.* [Internet]. 2012 [cited 2013 Sep 20]. Available from: http://www.comlaw.gov.au/Details/F2012L01703.

18. International Organization for Standardization. *ISO 27789:2013: Health informatics - Audit trails for electronic health records*. 2013. Available from: http://infostore.saiglobal.com/store/default.aspx.

19. Standards Australia. *ATS ISO 25237-2011: Pseudonymization*. 2011. Available from: http://infostore.saiglobal.com/store/default.aspx.

20. Australian Government. *National e-Authentication Framework.* [Internet]. [cited 2013 Aug 23]. Available from: http://agict.gov.au/policy-guides-procurement/authentication-and-identity-management/national-e-authentication-framework.

21. Australian Government. *Australian Privacy Principles, Schedule 1, Privacy Act 1988.* [Internet].Australian Government; 2014 [cited 2014 Jun 02]. Available from: http://www.comlaw.gov.au/Details/C2014C00076.

22. International Organization for Standardization. *ISO/IEC 27035:2011 Information technology - Security techniques - Information security incident management*. 2011. Available from: http://infostore.saiglobal.com/store/.

23. Office of the Australian Information Commissioner. *Data breach notification — A guide to handling personal information security breaches*. Australian Government; 2012. April 2012. Available from: http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches.

24. International Standards Organisation. *ISO 31000:2009 Risk management - Principles and guidelines*. ISO; 2009. Available from: http://infostore.saiglobal.com/store/default.aspx.

25. Standards Australia. *AS/NZS 5050:2010 Business continuity - Managing disruption-related risk*. 2010. Available from: http://infostore.saiglobal.com/store/.

26. Standards Australia. *HB 174-2003 Information security management - Implementation guide for the health sector*. Standards Australia; 2003. Available from: http://infostore.saiglobal.com/store/.