MINISTRY OF HEALTH
MANATŪ HAUORA

hiso
Health Information Standards Organisation
PAEREWA PĀRONGO HAUORA

HISO 10029:2015 Health Information Security Framework

ConnectedHealth
My information. Better care.

Document information

HISO 10029:2015 Health Information Security Framework is a standard for the New Zealand health and disability sector, published December 2015.

First published in September 2009 as HISO 10029.1-3 Health Information Security Framework.

ISBN 978-0-947491-48-2 (online).

Health Information Standards Organisation (HISO) is the expert advisory group on standards to the National Health IT Board (the IT Board).

HISO standards are posted on our website at http://healthitboard.health.govt.nz/standards

Contributors

Health Sector Architects Group
Canterbury District Health Board
NZ Health Partnerships Ltd
National Institute for Health Innovation
CSC Australia
Department of Internal Affairs
Patients First Ltd
Central TAS
HealthShare Ltd
Dimension Data

Copyright

Keeping standards up-to-date

HISO standards are regularly updated to reflect advances in health information science and technology. See our website for information about the standards development process. We welcome your ideas for improving this standard. Email standards@health.govt.nz or write to Health Information Standards, Ministry of Health, PO Box 5013, Wellington 6145.

New Zealand legislation

The following Acts of Parliament and Regulations have specific relevance to this standard. Readers must consider other Acts and Regulations and their amendments that are relevant to their own organisation, in the implementation or use of this standard.

- Crimes Act 1961
- Electronic Transactions Act 2002
- Health Act 1956
- Health and Disability Commissioner (Code of Health and Disability Services Consumers' Rights) Regulations 1996
- Health Information Privacy Code 1994
- Health Practitioners Competence Assurance Act 2003
- Injury Prevention, Rehabilitation, and Compensation Act 2001
- Mental Health (Compulsory Assessment and Treatment) Act 1992
- Privacy Act 1993 (revised 2008)
- Public Records Act 2005

Contents

1 Introduction

This second edition of the Health Information Security Framework supersedes the first edition (HISO 10029.1; 10029.2 and 10029.3). The 2015 version can be found on our website: https://healthitboard.health.govt.nz/standards/approved-standards

1.1 Purpose and background

A health and disability sector-wide Health Information Security Framework advises how health information is created, displayed, processed, transported, has persistence and is disposed of in a way that maintains the information's confidentiality, integrity and availability.

Confidentiality:	Access to health and disability information is limited to authorised users for approved purposes.
Integrity:	Data and information is accurate, consistent, authentic and complete. It has been properly created and has not been tampered with, damaged or subject to accidental or unauthorised changes. Information integrity applies to all information, including paper as well as electronic documents.
Availability:	Authorised users ability to access defined information for authorised purposes at the time they need to do so.

Threats concerning the confidentiality, integrity and availability of the health and disability sector's physical and logical assets must be identified, assessed, recorded, prioritised and managed.

The relationship of trust that exists between a patient and their health care provider is vital for good health care. The health care provider must treat personal health information with proper care and respect and to keep it secure. If information is disclosed inappropriately, corrupted or lost, the consequences for both patient and health care provider are potentially very serious.

Personal health information is used to deliver health care as well as to support the business of health care, teaching, research and population health management.

An organisation that does not have a health information security policy cannot assure patients their information is being treated and protected appropriately.

The Health Information Security Framework Standard (HISF) supports organisations preparation and maintenance of such a policy. The HISF provides advice about procedures and technical standards that need to be incorporated in a policy and sets out minimum requirements and desired goals at various levels of organisation operational complexity and risk.

As noted in section 1.4 Risk management, the framework is to be applied using a risk-based approach. For more information see Appendix D – Related specifications

1.2 Scope

The Health Information Security Framework is concerned with the security of health information wherever it may exist.

All references and annotations identified in this document are current at the time of publication. It is incumbent upon the reader of this document at the time of use to ensure that the references provided are up to date and relevant.

Health information privacy is covered by the Health Information Privacy Code, and is not within the scope of this document. Privacy is an outcome and relies on many mechanisms, only one of which is security.

This document assumes personal health information will be shared – it does not say what information is to be shared or under what circumstances (eg, where identifiable health information is anonymised). Restrictions on information sharing apply to personally identifiable information; health information that has been anonymised is not necessarily subject to the same sharing restrictions.

All patient-identifiable health care information is classified as 'MEDICAL-IN-CONFIDENCE'[1] and given an equal level of protection unless otherwise classified.

There are a number of security codes of practice in current use that focus on different parts of the health and disability sector:

- The Health Network Code of Practice published in 2002 by Standards New Zealand. This standard principally covers the security requirements for the transfer of health information over computer networks
- Aiming for Excellence. This covers some of the key elements of security of information in general practice. Aiming for Excellence is the Royal New Zealand College of General Practitioners' standard for general practice.

1.3 Health Information Security Framework Standard Application

The development and application of specific security policies and procedures to support the organisation is the responsibility of the organisation's management. However, compliance with the framework's Risk management section 1.4 **is required** from 1 July 2016.

The content of the framework, while comprehensive, is not exhaustive. Relying solely on the adoption and application of the framework without due consideration of the 'real world state' does not adequately discharge the management responsibility to provide and maintain health care information that has confidentiality, integrity and availability.

1.4 Risk management

Health care organisations must undertake the following three activities as a minimum to meet their responsibilities in managing health information.

1.4.1 Regularly undertake a (or review an existing) health information related risk assessment

Look specifically at the areas listed in this document as a minimum. While documenting risk assessment processes is out of scope for this framework, the assessment must cover the

[1] Refer the national security classifications as set out in the Protective Security Requirements and the New Zealand Information Security Manual – see Appendix D – Related specifications

following for each perceived risk (see ISO 31000 Risk Management and Appendix D – Related specifications):

- probability of the risk event occurring
- impact if the risk event occurs
- available risk mitigation actions and counter-measures.

1.4.2 Develop and apply policies and procedures to address each of the identified risks

See the relevant sections of this framework for more information.

1.4.3 Regularly monitor and report on the performance of the above policies/procedures

This includes reviewing each policy/procedure for effectiveness and updating the policies/procedures as needed.

In summary, the provision of appropriate effective health information security:

- is a requirement of management
- must be tailored to the individual requirements and exposures faced by each health care organisation.

The Health Information Security Framework provides guidance, ideas and comment to support these tasks.

1.5 Health care organisation category definition

The Health Information Security Framework records the minimum areas of policy (and associated procedures) to be developed and applied by all health and disability sector provider organisations.

The requirements for each individual security section have been grouped into three organisation compliance categories. Organisations are required to attain at least the Baseline level for each section. Some organisations are required to reach Intermediate or Advanced level for some or all categories. For example: DHBs may be required to operate at Intermediate level for a category while GP practices may only be required to operate at a baseline level for the same function.

Note: Categories in the table below are additive. To attain an Intermediate level, an organisation must meet all Baseline and Intermediate criteria for that category. Similarly, to attain an advanced level, all baseline, intermediate and advanced criteria for that category must be met.

Organisation category	Category Indicators
Baseline	The procedures outlined in the Baseline category are the absolute minimum. Compliance with this level is required of all health care (or support) organisations operating in the New Zealand health and disability sector.

Organisation category	Category Indicators
Intermediate	Some organisations are required to achieve Intermediate level for some or all categories. This is based on the type of data they hold, functions they perform or a heightened level of risk they are exposed to.
Advanced	Some organisations are required to achieve Advanced level for some or all categories. This occurs when the type, quality or quantity of data they hold, or functions performed, expose them to a significantly high level of risk.

Note: The above are not the only category indicators. Organisation management is responsible for determining the risk profile for each individual information system or service. The organisation should then operate in a category or categories commensurate with that risk assessment.

While size, scale of operation and resourcing available to any particular organisation are important components for determining the category the organisation operates in for each information security aspect, they are not the only or key category determinates.

Further guidance on risk assessment can be found in the All-of-Government ICT Operations Framework and Information Security Risk Assessment Process - see Appendix D – Related specifications

All organisations must ensure they meet the Baseline level for all categories. Requirements for additional higher-level controls will be determined based on infrastructure and application risk assessments, or by way of compliance with a particular government mandate.

The procedures set out in each section apply to health care organisations and those operating under contract to them.

1.6 Information security – minimum areas of activity

The following sections in this document describe the objectives, policy requirements and procedures (within the three organisation compliance categories) that are applicable within the context of the Health Information Security Framework requirements (section 2.2 Framework).

Over time the areas discussed below will expand and potentially contract as information systems domains change. The absence from the framework of a particular newly developed domain or function does not state or imply there is no activity required in such areas. Management is expected to be proactive and investigate/manage security implications of health information developments as they occur.

As discussed in section 4 Information security policy, this document:

- does not remove the requirement on management to be responsible for their business. Management are expected to undertake risk assessments and make informed decisions
- is based on the ISO 27000 standards series. The Ministry of Health has a copyright licence to use parts of this ISO publication (Appendix D – Related specifications)
- does not contradict the New Zealand Information Security Manual, the New Zealand Protective Security Requirements, the Privacy Act or other New Zealand legislation or regulations.

1.7 Information security – high-level consideration

In addition to the material described in the various sections below, there are a number of fundamental approaches that must be adopted and applied by all health and disability sector organisations. These comprise (no implied priority or order):

- all patient identifiable information must be protected at rest and in transit
- whilst the application of security passwords is discussed in the various sections below, it is important to understand that the device involved is not the only driver of the need to apply password protection. It is the information that is being held or the ability of the device to access information on another device that is the key point of concern.

1.8 Responsibility for health information security

- Health care organisations are responsible for reducing or mitigating risks to their assets. They must show a clear understanding of the risks to and potential impacts on information security that the organisation faces. This applies to day-to-day operations, as well as to major failures of information systems or other disruptive events.
- Every employee, consultant or contractor in the health and disability sector has responsibility to maintain day-to-day security of all sites, services, systems and information.

People in the following positions have the main responsibility for information security within the health and disability sector.

- Minister of Health
  Has overall responsibility for the security of information assets. The Ministry of Health acts on behalf of the Minister.
- Chief executive (CE)
  Has overall accountability for the operations of the organisation, including information protection and assurance activities.
- Chief information security officer (CISO)
  Responsible for managing the security strategy and approving the supporting security policies and control measures.
- Information technology security manager (ITSM)
  Acts as a conduit between strategic directions from the CISO and their implementation by system administrators. Their main area of responsibility is administrative and process controls relating to organisation information security[2].
- System and information owners and their delegates
  Responsible for ensuring security requirements are adequately addressed during the design, development and implementation or operation of any existing, new or altered information systems. They must also maintain system accreditation.
- System users
  Have responsibility to comply with this information security policy and other supporting documents within and relevant to their role.

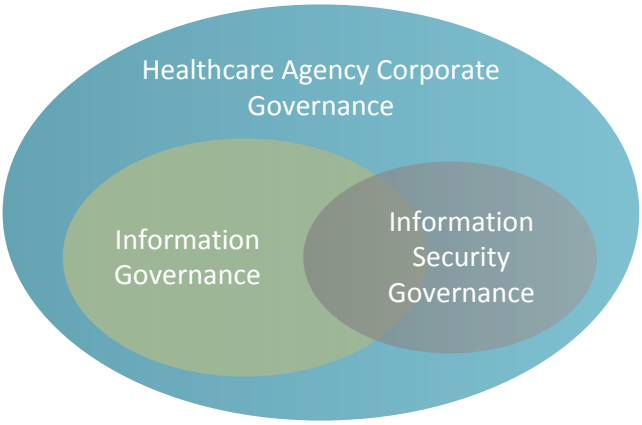
[2] NZISM V2.3 Section 3.3.3

2 Health information governance and management

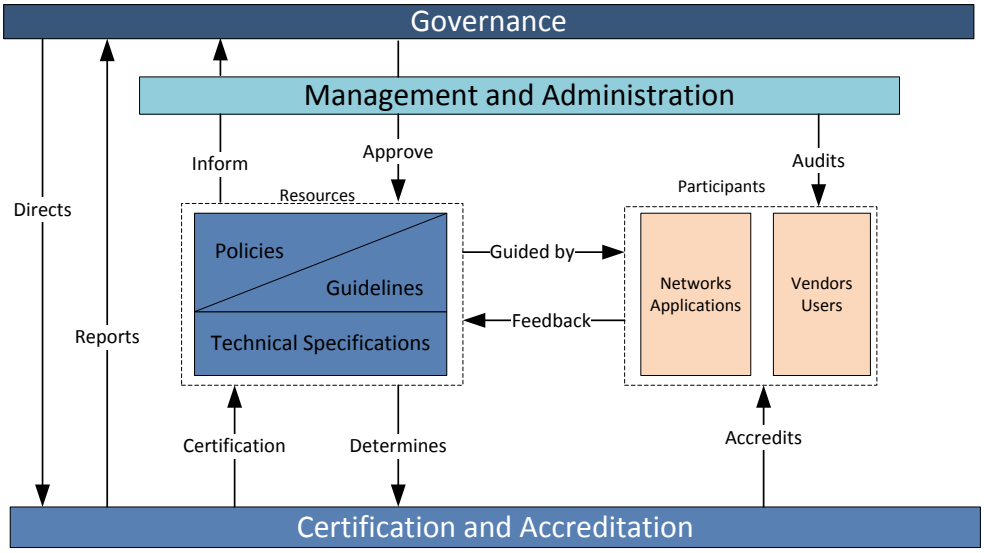
2.1 Background

Governance has been described as "the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are suitably managed and verifying that the enterprise's resources are used responsibly"[3]. Information security governance is a subset of governance.

Corporate information and security governance



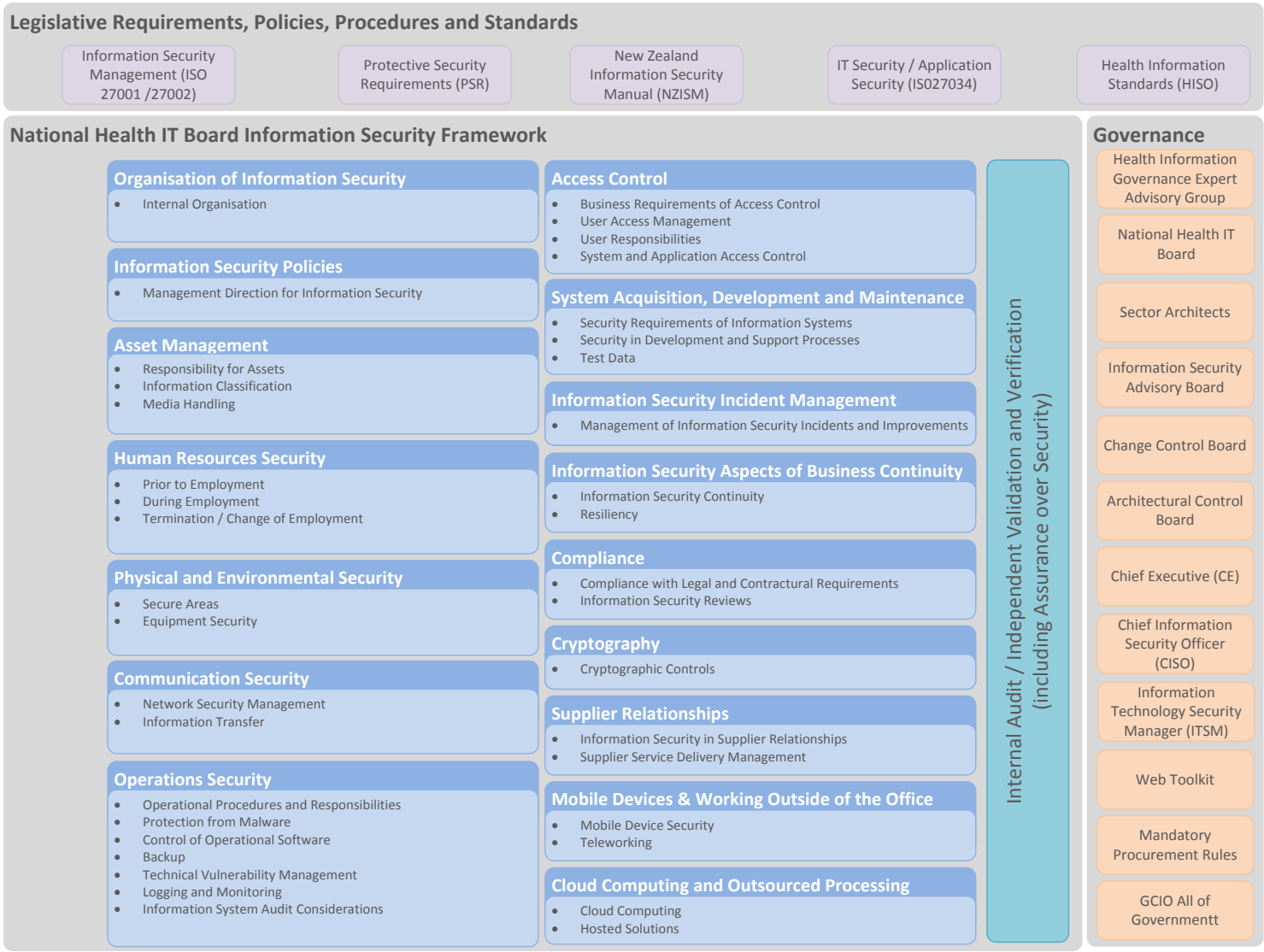
Core governance and management relationships and their interactions in the New Zealand health and disability sector are shown below. Note that networks and applications are accredited, while vendors and organisations are audited.



[3] IT Governance Institute, Board Briefing on IT Governance, 2nd Edition, USA, 2003, www.itgi.org

2.2 Framework

The diagram below shows the areas addressed by this framework.



2.3 Governance

Health care organisations are required to have a governing body made up of health and disability sector representatives, and consumers.

Governance provides the key elements that deliver effective:

- risk management assessment, analysis and mitigation plans
- implementation of systems that ensure 'security by design' is embedded into the culture of the organisation
- leadership, oversight and monitoring of resulting changes.

Governing bodies have a role in ensuring:

- this framework:
  - is widely promoted and adopted in the health and disability sector
  - supports a 'living' standard, where elements of interpretation and clarification can lead to incremental and on-going improvements.
- their organisation complies with the framework.

Health care organisation tasks that may provide support to perform framework and governance body functions include activities such as:

- overseeing health and disability sector organisations' and vendors' transition activity to achieve compliance
- developing and implementing security audits
- resolving disputes and matters of interpretation
- maintaining and updating a technical specifications register
- determining consequences for non-compliance
- provision of security advice, training and implementation support for small organisations.

The governance function:

- is supported by management and administration
- assists with developing and maintaining the health information security framework and associated standards, including providing well-researched security-related policy advice
- provides training and support services to sector organisations and projects to ensure the security framework is understood, meets the needs of users and is being used appropriately and consistently
- monitors and reports on the status of authentication and security within organisations holding health information.

3 Organisation of information security

3.1 Objective

Establish a management framework to develop, initiate and control the implementation and subsequent operation of information security within the health care organisation.

In every organisation, responsibility for managing health information security requirements needs to be clearly defined and reside with at least one senior individual. All staff must be aware of the security responsibility undertaken by that nominated individual or individuals.

3.2 Policy requirements

Policy is required to research, consider, approve, formally document, audit, regularly review and enforce procedures to address:

- setting the information security roles and responsibilities - see NZISM 'Appointing a CISO' about managing conflicts of interest
- segregation of duties
- contact with authorities
- contact with special interest groups
- information security in business requirements.

3.3 Procedures

3.3.1 Baseline procedures

Responsibility	Procedure description
Management	• Information security officer responsibility is formally assigned. • Practical segregation of duties, requirements and opportunities are identified and applied. • Legally enforceable contracts are developed and applied. • Information security principles are incorporated into business requirements.
System administrator	No additional requirements in this section
User	No additional requirements in this section

3.3.2 Intermediate procedures

Responsibility	Procedure description
Management	• Ensure the information security officer responsibility is not assigned to a position with IT operational responsibilities, such as an IT administrator. • If feasible, the information security officer should report through a risk, compliance or other appropriate division of the organisation outside of IT. • The information security officer should understand IT and the organisation's accepted risk tolerance. They should work towards implementing information security requirements that are in line with the accepted risk tolerance, while complying with required legislation, regulation or other requirements. • Detailed segregation of duties requirements and opportunities are identified, applied and monitored.
System administrator	No additional requirements in this section
User	No additional requirements in this section

3.3.3 Advanced procedures

Responsibility	Procedure description
Management	The information security officer role is assigned to an executive within the governance/management group, excluding the CIO or equivalent.
System administrator	No additional requirements in this section
User	No additional requirements in this section

4 Information security policy

4.1 Objective

Set the tactical direction for information security in an organisation through documented information security policies.

4.2 Policy requirements

Information security policies are to address requirements created by:

- business strategy
- regulations, legislation and contracts
- current and projected information security threat environment.

Some consolidation of policies may be warranted depending on the mix of individual organisational security risks and requirements.

4.3 Procedures

4.3.1 Baseline procedures

Responsibility	Procedure description
Management	• Organisations must have an information security policy to meet the needs of their organisation that is reviewed and updated at least annually. • The information security policy must address security principles, security responsibilities, and an 'acceptable use policy' for any organisation technology equipment, systems, resources and data. • An information security policy document must be approved by management and published, reviewed and communicated regularly to all employees and relevant external parties.
System administrator	Ensure that all employees are aware of the information security policy and kept informed of any changes and updates.
User	Read, review, understand and follow obligations under the information security policy.

4.3.2 Intermediate procedures

Responsibility	Procedure description

Management	• Organisations must:
	  ○ have an information security policy that establishes the overarching security principles and control objectives for the Information Security Management System (ISMS) based on the ISO/IEC 27002 Framework (see Appendix D – Related specifications)
	  ○ establish clear lines of responsibility for information security
	  ○ embed information security into everyday practice by clarifying the actions required of all staff to protect the organisation's information assets and information and communications technology (ICT) assets
	  ○ ensure every system is covered by a security risk management plan. Such a plan is considered to be a best practice approach to identifying and reducing potential security risks
	  ○ ensure there is a system security plan describing the implementation and operation of controls within the system derived from the NZISM and the security risk management plan
	  ○ ensure standard operating procedures are developed for systems. These provide step-by-step guides to undertaking information security related tasks and processes. They provide assurance tasks can be undertaken in a secure and repeatable manner, even by system users without strong technical knowledge of the system's mechanics.
	• The information security policy is usually sponsored by the chief executive and managed by the chief information security officer or chief information officer. The IT security manager must be the custodian of the policy.

System administrator	No additional requirements in this section
User	No additional requirements in this section

4.3.3 Advanced procedures

Responsibility	Procedure description
Management	No additional requirements in this section
System administrator	No additional requirements in this section
User	No additional requirements in this section

5 Asset management

5.1 Objectives

- Identify assets belonging to the organisation and define and allocate responsibilities for the protection of these assets.
- Ensure assets receive protection based on their importance to the organisation.
- Ensure assets are continuously maintained to an appropriate security baseline that minimises their vulnerabilities and threat exposure, such as regular patching and other activities (see also Section 9 – Operations security).
- Prevent unauthorised disclosure, modification or destruction of information stored on media.
- Ensure assets are controlled and managed in accordance with best industry practice, notably at least aligned to the Information Technology Infrastructure Library (ITIL) Service Management framework.

5.2 Policy requirements

A suitable high-level policy will consider and address at least:

- responsibility for assets
- asset classification and declassification in terms of legal requirements, value, criticality and sensitivity
- media handling.

5.3 Procedures

5.3.1 Baseline procedures

Responsibility	Procedure description
Management	***Responsibility for assets*** • Create an inventory of information and information processing facilities assets. • Assign ownership of assets as they are created or transferred to the organisation. • Identify and document rules for the acceptable use of information and information processing facilities assets. • The termination process must be formalised to include the return of all organisational assets issued, both physical and electronic. • Establish procedures for handling, processing, storing and communicating information. • Establish procedures to interpret classification labels from other organisations where information is shared. ***Asset classification*** • An asset classification scheme is to be provided.

	• Create a set of procedures for labelling information and its related assets in physical and electronic format. ***Media handling*** • Establish procedures for the secure disposal of media. • Identify and document a set of rules and guidelines for protecting assets against unauthorised access, misuse or corruption during transportation. • Establish procedures for the management of removable media.
System administrator	***Responsibility for assets*** • Ensure assets are inventoried. • Periodically review access restrictions and classification of assets. • Inform employees and external parties of the security requirements relating to the assets they use. • Control unauthorised copying/printing of information during an employee's notice period. • Add access restrictions supporting the protection requirements. • Create and retain a formal record of authorised recipients of assets. • Protect both temporary and permanent copies of information. • Store IT assets in accordance with specifications from manufacturers. ***Asset classification*** • Label assets in accordance with predetermined and approved labelling procedures. ***Media handling*** • Prevent the use of media containing classified information with a system that has a security classification lower than that of the media. • Make copies of valuable data on separate media to reduce the risk of data damage or loss. • Move copies of valuable data to a different secure location to reduce the risk of data damage or loss. • Encrypt confidential data on removable media. • Ensure physical assets are sanitised (have information fully removed) prior to disposal. Paper or other physical media must be physically destroyed. • Implement rules and guidelines for protecting assets against unauthorised access, misuse or corruption during transportation. • Log and sanitise or destroy media containing sensitive information when it is no longer needed.
User	***Responsibility for assets*** • Conform to acceptable use of health information guidelines and security requirements. • Justify access to personal health information.

	• Return all organisational assets on termination of employment, contract or agreement. • Transfer and document important knowledge about ongoing operations to the organisation during the notice period of termination.

5.3.2 Intermediate procedures

Responsibility	Procedure description
Management	Identify, document and manage the asset/assets' lifecycle.
System administrator	No additional requirements in this section
User	No additional requirements in this section

5.3.3 Advanced procedures

Responsibility	Procedure description
Management	No additional requirements in this section
System administrator	No additional requirements in this section
User	No additional requirements in this section

6 Human resources security

6.1 Objective

Ensure employees, contractors and third party users conform to the organisation's health information security policy and procedures.

Individuals play the most crucial role in the protection of personal health information. Patients expect their health information to be maintained confidentially and securely by those authorised to use it.

Additional human resource policy and supportive documentation is provided by the Protective Security Requirements and the New Zealand Information Security Manual– see Appendix D – Related specifications

6.2 Policy requirements

All human resource policies and procedures, including relevant contractual terms and conditions, must incorporate information security requirements.

6.3 Procedures

6.3.1 Baseline procedures

Responsibility	Procedure description
Management	***Screen new staff*** • Ensure new employees, temporary staff and contractors are screened in relation to their appointed task. ***Contracts & job descriptions*** • Include health information security responsibilities and non-disclosure agreements in job descriptions, contracts of employment and contracts for service, and induction material. • Ensure all users receive relevant health information security awareness training. ***Role membership assignments*** • Authorise all role membership additions and changes, and associated information security permissions prior to implementation. ***Disciplinary process*** • Introduce, communicate and maintain a formal disciplinary process for employees responsible for health information security breaches.
System administrator	***Maintain user access rights*** • Follow documented recruiting and termination procedures for creating and removing users' access rights. • Ensure that a user's access rights are regularly reviewed and amended accordingly on changes of role and/or accountabilities within the organisation.

	• Ensure the return of all equipment and removal of all information security permissions on termination of employment or service contract, or on request. ***Maintain security policy documentation*** • Ensure the organisation has documentation matching current security legislative and policy requirements. • Ensure a security policy responsibility agreement is signed by all employees and contractors. ***Security auditing*** • Implement role-based security to maintain access authorisation rights.
User	***Course of engagement*** • Act in accordance with all relevant health information security policies and procedures. • Be aware of how to report a health information security incident. ***Sign security policy responsibility agreement*** • At the time of engagement, personnel sign a security policy responsibility agreement to show they have read, understood and accepted the health information security policy. ***Exit procedures*** • Return all related assets (including hardware, software, information processing and storage devices, printed material or other hard copies) when leaving the organisation or role.

6.3.2 Intermediate procedures

Responsibility	Procedure description
Management	***Awareness training*** Ensure all parties receive regular and appropriate health information security awareness education and training relevant to their job.
System administrator	***Maintain user access rights*** • Ensure all users receive relevant health information security awareness training as soon as possible. ***Security auditing*** • Ensure information systems record all unauthorised access attempts. • Regularly review the system audit trail record of all unauthorised access attempts. Report and take action as needed. • Record the date/time/source (both system and user) of all changes made to sensitive data, including inserts and deletions, and the identity of the user who made each change.
User	***Engagement*** Sign a contract of employment, or contract for services that includes health information security responsibilities.

6.3.3 Advanced procedures

Responsibility	Procedure description
Management	Ensure the organisation's access management systems use an authoritative information source(s).
System administrator	***Maintain user access rights*** • Ensure users have received relevant health information security awareness training before they are provided with any information security access rights and credentials. ***Security auditing*** • Periodically review the system audit trail of new users and users with recently re-assigned security roles. • Ensure information systems record all authorised accessing of confidential data.
User	***Attend induction course*** Ensure personnel attend an induction course which covers health information security awareness, education and training relevant to their position accountabilities.

7 Physical and environmental security

7.1 Objective

Prevent unauthorised physical or electronic access to the organisation's information assets and information processing facilities. This will guard against loss, damage, theft, interference or compromise of assets, and interruption to the organisation's operations.

7.2 Policy requirements

Establish a suitable high-level policy and controls to meet the objective. Additional policy and supportive documentation on the physical dimension is provided in the Protective Security Requirements and the New Zealand Information Security Manual– see Appendix D – Related specifications

Procedures

7.2.1 Baseline procedures

Responsibility	Procedure description
Management	***Secure areas*** • Define security parameters. The siting and strength of each depends on the security requirements of the assets within the organisation's perimeter and the results of a risk assessment. • Secure areas that contain personal health information and information processing facilities by restricting or supervising physical access. • Ensure there are adequate locks on all access doors. Place bars or security locks on windows. Maintain a record of who has the keys. • Provide secure offices, rooms and facilities and reasonable protection against damage from fire, flood, earthquake or other forms of environmental hazard. • Preauthorise off-site use of equipment, software or information. • Make provision for private areas where sensitive information can be discussed. • Install a working burglar and fire alarm system and test them regularly.
System administrator	• Check information storage to ensure any health information and software is rendered non-retrievable prior to disposal or re-use. • Maintain and regularly check equipment to ensure its continued availability and fitness for purpose. • Protect the perimeters of buildings or sites containing information-processing facilities against unauthorised access using suitable physically sound external doors with control mechanisms.
User	• Do not discuss or leave printed personal health information in a place where unauthorised users may overhear or see it. • Work in a secure area when necessary for the task in hand.

	• When working off-site, at home or in other public areas, use of portable computers and storage media must be operated in accordance with a 'use of portable devices' policy.

7.2.2 Intermediate procedures

Responsibility	Procedure description
Management	• Establish and operate a staffed reception area or other means to control physical access to the site or building. • Establish physical barriers to prevent unauthorised physical access and environmental contamination. • All fire doors on a security perimeter must be alarmed, monitored and tested in conjunction with the walls to establish the required level of resistance in accordance with suitable regional, national and international standards. They must operate in accordance with the local fire code in a failsafe manner. • Maintain and monitor a secure physical log book or electronic audit trail of all access. • Organisations must have controlled room(s) to hold critical computer equipment (servers, network).
System administrator	• Access rights to secure areas must be regularly reviewed and issues taken to management for action. • Storage media containing personally identifiable information must be sanitised when the asset is being decommissioned. • Control and monitor access to restricted areas electronically, eg, via card system or camera.
User	• Report broken or malfunctioning equipment to management.

7.2.3 Advanced procedures

Responsibility	Procedure description
Management	• Information processing facilities managed by the organisation must be physically separated from those managed by external parties.
System administrator	• All employees, contractors and external parties must be required to wear a visible form of identification. Any unescorted visitors and/or anyone not wearing visible identification must be immediately reported to security personnel. • All incoming and outgoing shipments must be controlled.
User	No additional requirements in this section.

8 Communications

8.1 Objective

Ensure the integrity of information communicated across networks and that any changes are authorised and controlled.

8.2 Policy requirements

Policies are required to address at least (but not limited to) the categories listed below.

Connections policy

The organisation has formally documented:

- the types of systems/devices that may be attached to the network(s) and in what manner this attachment can occur
- the types of systems/devices that are not permitted on the network
- any other prerequisite requirements that must be met before connection occurs.

Information transfer policy

The organisation has formally documented:

- the minimum technical standards for packaging and transmission of health information
- the tools to be used for the transmission of information between organisations or sections/business units of the organisation
- how personal health information exchanged over a network is protected from interception, incorrect routing and/or loss
- how personal health information exchanged on physical media is protected from unauthorised access, misuse or corruption
- agreed requirements with external parties, relating to transferred personal information
- responsibilities and liabilities in the event of information security incidents
- incident notification requirements
- labelling for sensitive data
- use of security controls such as Cryptography and cryptographic key management (see section 15).

Information protection policy

The organisation has formally documented policies addressing:

- detection of malware during transmission
- patient data leakage
- attachment of inappropriate information
- copying/modification and destruction
- tools supported for the transfer of information.

8.3 Procedures

8.3.1 Baseline procedures

Responsibility	Procedure description

Management	***Policies, procedures and standards***
	• Create policy documents on:
	  ○ connections
	  ○ information transfer
	  ○ information protection.
	• Ensure users:
	  ○ are aware of their responsibilities when transmitting information
	  ○ know the location of and can access the relevant policies, agreements and procedures
	  ○ clearly identify mediums and types of sites that can be used for the different types of information being transmitted.
	• Ensure formal confidentiality or non-disclosure agreements are in place with external parties that receive personally identifiable data. The agreement(s) must cover vendors/contractors dealing with the recipient organisations and include:
	  ○ definitions of information to be protected
	  ○ duration of agreement
	  ○ process for notification of leakage
	  ○ ownership
	  ○ the right to audit and monitor activities that involve personal information.
	• Ensure formal service level agreements are in place to cover at least the:
	  ○ main components that support the network infrastructure
	  ○ inclusion in the contract of the right to audit.
	• Ensure all agreements and policies are regularly reviewed at least yearly and updated as required.
	• Ensure appropriate electronic signatures containing legal disclaimers are used for electronic messaging.
	• Assign roles and responsibilities for network equipment management.

System administrator	***Management/monitoring*** • Ensure all networking devices default accounts have their passwords changed, and default account names are renamed. • Ensure all networks are sufficiently documented including documentation of updates incorporated via the change management process. • Ensure network documentation includes up to date diagrams. • Ensure access to network services and equipment follow the procedures outlined in Section 10 Access control.

	• Ensure the HISO interoperability standards are followed for the exchange of health information within and between organisations. • Use appropriate encryption standards (see Section 15 Cryptography and cryptographic key management), when exchanging health information between external parties. • Ensure the communication of private information such as credentials are not sent via the same mechanism where more than one part exists. For example, send the username via email and the password via text – in both cases suitable encryption is required.
User	No additional requirements in this section

8.3.2 Intermediate procedures

Responsibility	Procedure description
Management	No additional requirements in this section
System administrator	***Management/monitoring*** • Implement technology that can monitor the status of network devices. Ensure monitoring is configured in a secure way (ie, no default community strings, no older Simple Network Management Protocols). • Implement technology that centralises the management of access control to networking components. • Establish and maintain appropriate network security zones, allowing data flow to follow a controlled path only. • Ensure only trusted devices and users can gain access to internal networks via wireless access. • For custom-developed applications, ensure the exchange or transfer of information between systems uses the appropriate interoperability standards. • Ensure network appliances are configured to support the segregation of networks. • Provide the appropriate level of protection to devices and information.
User	No additional requirements in this section

8.3.3 Advanced procedures

Responsibility	Procedure description
Management	No additional requirements in this section
System administrator	***Management/monitoring*** • Document and implement tools to enable the detection and prevention of unauthorised information transfer. • Ensure only trusted devices and users can gain access to internal networks.
User	No additional requirements in this section

9 Operations security

9.1 Objective

Ensure appropriate controls are implemented to protect the operational integrity and recoverability of the organisation's IT applications/information.

9.2 Policy requirements

A suitable high-level policy will consider and address:

- the organisation's requirements for the backup of information, software, and systems. This must include the level of protection required for the different categories of systems and the expected retention of the data being protected
- the IT response to a disaster event and where it sits in the organisation's business continuity plan
- the removal or upgrade of unsupported legacy software
- protection against malicious software such as malware, ransomware etc, is implemented
- requirements for the frequency and type of testing of information, software, and system integrity.

It is recommended organisations investigate an internationally recognised IT operational management framework such as Information Technology Infrastructure Library (ITIL) as a possible support tool for the above. ITIL provides current international best practice for the effective operation of an organisation's IT environment – see Appendix D – Related specifications

9.3 Procedures

9.3.1 Baseline procedures

Responsibility	Procedure description

Management	***Procedures and standards***
	• Ensure all systems have documented operating procedures that are made available to all users.
	• Provide ongoing awareness updates for users on how to lessen the likelihood of a malware attack, by focusing on avoidable user behaviours.
	• Create an accessible and available operating procedures manual(s) that documents:
	  ○ backup and recovery procedures
	  ○ computer start-up and close down procedures
	  ○ system restart and recovery procedures
	  ○ equipment maintenance functions
	  ○ change management
	  ○ instructions for handling errors
	  ○ management of audit trail and system log information

	○ management of a security event, including a physical security breach or one associated with a malware or hacking breach. • Ensure appropriate operating procedures are created, implemented, and maintained to protect documents, removable storage media, printed information and system documentation from unauthorised disclosure, modification, removal and destruction. • Ensure systems are monitored, with operator and fault logs checked regularly to ensure information system problems are identified and corrected. ***Change management*** • Plan and test changes before implementation. • Assess all potential impacts and risks. ***Protect information*** • Ensure data is adequately backed up and stored in a protected location.
System administrator	***Protect information, systems and networks*** • Implement anti-malware and anti-virus software on all servers and workstations. Ensure it is kept up-to-date. • Ensure real-time malware scanning is activated and scheduled scans are run on a regular (eg, weekly) basis. • Ensure appropriate backups (type and frequency) are implemented based on the return to operation category for each information software/system. • Ensure the backup process includes type, retention, frequency and remote storage. ***Patching/firmware*** • Ensure there is at least one person in the organisation keeping up to date with current threats and ensuring the correct mitigation is in place. • Apply all critical security patches as soon as practical from the date of release. ***Management, monitoring and alerting*** • Implement technology that can detect and prevent access to malicious websites or sites from prohibited categories. • Ensure all systems are sufficiently documented, including documentation of updates that are incorporated via the change management process. • Ensure system documentation includes up-to-date diagrams.
User	***Report problems*** • Be aware of the dangers of viruses and malware and report suspicious events to management immediately.

9.3.2 Intermediate procedures

Responsibility	Procedure description

Management	***Operations procedures***
	• Track systems and their configuration information in a configuration management database.
	• Develop a formal policy around the installation and use of unauthorised software, and ensure technology and processes are implemented to enforce this policy.
	• Ensure a system and software lifecycle policy is defined in accordance with the organisation's risk tolerance profile.
	Protect information, systems and networks
	• Ensure networks are managed separately from other operations.
	Change management
	• Establish and apply a formal process:
	  ○ to control all changes and appropriately authorise all significant changes to systems and networks
	  ○ for emergency changes when incidents occur.
	• Ensure all change processes are reviewed at least bi-annually and updated as required.
	• Ensure back-out/recovery plans are fully documented, incorporating procedures for when a back-out/recovery is required.
	• Ensure all assets are registered in an asset management system. The system must be able to dynamically update details regularly using agent software or similar.
	• Ensure a process exists for the adoption of systems from development or project mode to operational status. This includes the development of formal documentation to enable support of the system to the agreed service levels.
	People management
	• Segregate access rights to reduce opportunities for misuse of information assets.

System administrator	***Information security***
	• Provide and maintain the ability to:
	  ○ write data to portable storage media in an encrypted format
	  ○ securely "wipe" data/information stored on hard disks before their re-use or disposal.
	• Formally document operating procedures, including how to dispose of media safely and how to encrypt data on portable media.
	Protect information, systems and networks
	• Ensure archived or stored data is kept in a secured (encrypted) but open format that is readable and retrievable after 10+ years.

	• Ensure anti-malware products from more than one vendor are installed across the organisation. For example, desktops and laptops have anti-malware products from vendor 'A' while server's anti-malware solution is from vendor 'B'. • Ensure adequate backup/restore computing and storage resources are available to recover all critical systems following a major event or media failure. • Implement a configuration control system to track versions/revisions of software implemented and their relevant documentation. ***Patching/firmware*** • Formally assign roles and responsibilities for vulnerability management including vulnerability monitoring, assessment and coordination responsibilities. • Document a formal process that outlines standard and urgent patch application, setting out the criteria that must be met before urgent patching takes place. • Ensure patches are deployed to a subset of devices to allow testing before deployment to all. • Where a vulnerability is known or identified but no patch is currently available, use other alternatives to mitigate risk (such as firewall controls to limit functionality or restrict access), and prevent execution of suspect executable files. • Ensure firmware on devices is updated at least yearly, with a more regular requirement if security vulnerabilities are behind the reason for the update. • Where devices are no longer supported and software updates are not available, a risk assessment must be performed to determine the impact of an incident and the increased vulnerability. ***Testing*** • Test new versions of software and features before deployment. • Require vendors to produce or show evidence of adequate testing, before deploying new versions and features, or provide on-site test facilities to enable pre-deployment testing to take place. • Develop suitable acceptance test scripts for systems during changes and upgrades to systems. • Document and apply clear processes for the transfer of information/software between test/development and production environments. • Ensure sufficient separation exists between test/development and production environments to reduce the risk of accidental changes to the production systems. • Ensure testing is never performed on production systems. • Ensure different user profiles (with permissions appropriate for the tasks) are used for operating, testing and using systems.

	• Do not allow development tools or editors to be installed onto production systems. • Regularly validate backups by performing an isolated recovery. ***Capacity management*** • Ensure there is sufficient capacity with information systems to support good system performance and reliability. • Ensure critical systems have capacity management procedures. • Enable monitoring of capacity management to ensure performance or function is not affected by insufficient resources • Understand the potential effect of the forward pipeline of projects or expansion that requires resources so capacity can be managed appropriately. • Ensure processes exist to regularly: o decommission systems that are not required o optimise databases o archive data that is not accessed regularly. • Ensure that in the event of a failure, sufficient priority and resource allocation is given for production to resume before test/development systems. ***Time management*** • Enable the ability to synchronise system clock(s) to an agreed accurate time source. • Disable the ability to change time on the local device. ***Monitoring and alerting*** • Maintain and operate an ability to log and/or alert data integrity faults generated by the system. • Ensure logging is occurring for the following activities: o changes to system configuration o the activation/deactivation of prevention systems such as malware protection.
User	***Protect information*** • Ensure physically stored media, including that stored or transported off-site, is encrypted. • Ensure data is classified correctly so the appropriate retention policy can be applied. ***Change management*** • Ensure any changes to systems or software receive formal management approval prior to implementation.

9.3.3 Advanced procedures

Responsibility	Procedure description
Management	***Operations policy*** • Ensure clear service level agreements are created with the business owner(s) for each category of system/service implemented and operated by the organisation. • Ensure the service level agreements clearly state what constitutes an IT disruptive event for the organisation. • Ensure administrators cannot disable, modify or erase activity logs. • Implement the 'Top 4 mitigation strategies to protect your ICT system' and the (Top 35), to minimise opportunities for unauthorised users tampering with properly configured cryptographic systems. http://www.asd.gov.au/infosec/mitigationstrategies.htm http://www.asd.gov.au/publications/Mitigation_Strategies_2014.pdf
System administrator	***Monitoring/alerting*** • Ensure log file information is protected for audit purposes, based on the established log tracking timeframes. • Detect and notify the asset management function of the installation of unauthorised software. • Enable logging of administrator/operator accounts and review regularly. • Perform regular checks to ensure access to systems and networks are secure, for example: penetration tests and vulnerability assessments.
User	No additional requirements in this section

10 Access control

10.1 Objective

Exercise sufficient control over health care information and therefore prevent unauthorised access.

Access control will help stop unauthorised persons accessing health information, ensuring it remains confidential. Authorised users will be able to view and process only the information they are entitled to and have a need to access.

10.2 Policy requirements

The organisation's identity and access management framework or system will define user access controls. The level of access control policy required will vary depending on the individual health care organisation.

Documented access control policy

The organisation has formally documented the following:

- **Category: Baseline**
  - the authoritative source for user data; including allocated role(s), location(s), devices and other attributes required to support corporate and health care systems
  - standard user access profiles for common job roles within the organisation
  - formal authorisation process for user account creation/deletion and access requests/removal (this may be part of the information security policy)
  - Access rights based on a 'least rights' model and 'prior to access' approval. The approver understands what they are granting access to
  - Along with terms and conditions of employment, there is a mechanism to ensure users sign an agreement that covers information confidentiality and disclosure
  - a process to ensure:
    - access control policies are regularly reviewed and updated where necessary
    - systems and applications that require authentication (as per the access policy) have a secure logon mechanism in place
    - utility programs or tools that may be capable of overriding system and application controls are restricted and tightly controlled.
  - Access to all accounts used for handling and management of patient-identifiable information, regardless of the device used, are to be restricted to that purpose. For example: coupling or automated linking of those user accounts to social media sites on the internet is not acceptable.
- **Category: Intermediate**
  - privileged user accounts (administrator rights) are only used for the special activities requiring their use, and not for day-to-day activities or over-ride access

- external support staff are only setup with temporary access rights for a fixed period and their accounts are set to expire at the end of that period
- external support staff accounts are separated from internal staff accounts for easier identification and management
- all users of health systems have uniquely identifiable accounts assigned to them to ensure individual responsibility. Generic accounts can be used to provide access to basic desktop functions, but access to health care and administrative applications require users to logon using their user identifiable accounts
- the reuse of user accounts is not permitted
- a separate authorisation process for the management of systems/information, over just standard user authorisation, is required
- ensure:
    - relevant contractual or legislative obligations are met for the access to data and services, particularly for privacy requirements
    - access control policies are regularly reviewed and updated where necessary.

- **Category: Advanced**
    - ensure there is segregation of the access control roles so the same person is not performing more than one of these roles – access request, access authorisation, access administration.

Clear desk and screen policy

The organisation has formally documented:

- a 'clear desk and screen' policy to protect paper and information on computer displays being seen by those who should not have access to the information.

Password policy

The organisation has formally documented:

- enforcement of passwords to a required complexity level based on the risk profile of the users and the information they have access to
- password complexity for privileged accounts (administrator access) that exceeds the password complexity required by standard users
- enforcement of password changes at regular intervals as required by the information security policy
- prevention of reuse of previous user passwords for a defined period of time eg, 13 months
- enforcement of access lockout after a fixed number of incorrect login attempts
- enforcement of access control measures (passcode etc) on mobile devices.

10.3 Procedures

10.3.1 Baseline procedures

Responsibility	Procedure description

Management	***General procedures***
	• Create policy documents covering:
	  ○ access control
	  ○ clear desk and screen
	  ○ password management.
	Audit
	• Undertake regular six-monthly audits of access logs, especially for privileged accounts.
	• Ensure all access allocation is documented and traceable.
	• Have a mechanism to allow verification that the level of access granted is appropriate.

System administrator	***Maintain access rights and password policies*** • Allow users to select and change their own passwords and include a confirmation procedure to allow for input errors. • Ensure users' access rights are appropriate to their task and are authorised and removed or modified upon termination of employment or change of role. • Ensure users are only able to access the resources and services required to carry out their duties. • Ensure access to program source code is restricted. ***Password protection*** • Store and transmit passwords in an encrypted non-reversible format eg, hash. ***Secure wireless networks*** • Ensure any wireless access points on the internal network are secured. ***Session protection*** • Automatically close down or terminate a session after a fixed time period of user inactivity (maximum of 15 minutes) or provide a locked screensaver option where the user must re-authenticate to unlock the system. • Ensure users cannot disable the locking mechanism.

	Policy notification • The system will display a logon banner that requires the user to acknowledge and accept their security responsibilities before access to the system is granted. Users must also be made aware that it is possible system usage is being monitored and the ramifications for violation of the relevant policies. Organisations must seek legal advice on the exact wording of logon banners. • Links to the full set of company policies must be easily accessible to all users.
User	***Good password practice*** • Follow good practice in the selection and use of passwords. • Do not share or disclose passwords. • Do not keep a record of passwords using a non-secure method such as on accessible paper, in a standard file or on a mobile device. • Change your password regularly per the password expiry standard defined in the information security policy or if you have any reason to suspect your password has been compromised/is known. ***Act responsibly*** • Read, review and understand obligations under the access control policy (such obligations may be included in the user's signed security agreement). • Accept responsibility for all access under their credentials and ensure access is related to their duties (and notify if it is not). • Do not leave the computer unlocked while unattended. • Report any security breach. • Prevent any inadvertent or unauthorised release of information, particularly from unattended equipment, by terminating active sessions, locking the screen or logging off when finished. • Close down/log off the computer at the end of the day.

10.3.2 Intermediate procedures

Responsibility	Procedure description
Management	***Policy*** • Extend the access control policy to meet this section's objective.
System administrator	***Secure networks and devices*** • Password-protect and encrypt information on devices used off-site, including laptops, mobile devices, home computers or portable media. • Support access to a secure network. • Password information must not be communicated to users via unencrypted emails. ***Session logging*** • Configure systems to display the date and time the user last logged in to assist in identifying unauthorised use of their account. • Remove or disable utility programs that are not required. ***Monitor & audit*** • Monitor for repeated account lockouts. ○ Keep an audit trail of all login attempts to the system – including successful login activity. The log should include at least user identifier, date, time, location, and duration of all user activity within an application (including view-only activity). • Allow viewing and analysis of audit trail activity by approved users. Restrict and record the ability to delete or modify log files. • Regularly review audit trails of access and activity – perform in depth audits and pay special attention to privileged accounts and external parties. ***Access control*** • Develop and operate a procedure to provide and revoke access rights at short notice, to support the requirements of locums and others for temporary access. • Access the Internet via a firewall or centralised device that monitors use and prevents access to unwanted material. • Maintain a telework and mobile devices register.
User	***Good password practice*** • Do not use the same passwords for personal and work related purposes. ***Act responsibly*** • Comply with section 17 Mobile devices and working outside the office.

10.3.3 Advanced procedures

Responsibility	Procedure description
Management	***Policy*** Extend the access control policy to meet this section's objective.
System administrator	***Access control*** • Implement tests for user proximity. The request to access information must be for a record that is, for example, recent in both time (looking at reasonably current information – not 'old') and physical location (nearby geographic information). • Do not disclose system or application identifiers until logon successful. • Applications must enable control of user access rights at each level of access, eg create, read, write, modify, delete and execute. • Applications must use menus or tabs to control (or hide) access to application system functions. ***Advanced authentication*** • Use multi-factor authentication to control access for remote users. • Where strong authentication requirements are identified, use alternatives to passwords such as biometrics, cryptography, smart cards and tokens. • Minimise access times to high-risk systems to reduce the window of opportunity for unauthorised access.
User	***Good password practice*** Do not use passwords that consist of words included in dictionaries.

11 System acquisition, development and maintenance

11.1 Objective

Ensure health information security is an integral part of the information system lifecycle.

Security is one outcome of good software design and development practices. This section relates to solutions developed/hosted 'on site', or that provide a service over a public network, including mobile applications.

Further guidance on the topic of risk assessment can be found in the all-of-government information security risk assessment process – see Appendix D – Related specifications

11.2 Policy requirements

In the context of software development and maintenance, the user is likely to be a software development professional, such as an architect, designer, developer or tester. All software development projects (whether internal, out-sourced or purchased products) related to the capture, display, processing, exchange and persistence of sensitive information, must incorporate industry best, and secure, practices.

While mobile applications present risks and hazards not necessarily found in traditional centralised computing, from a development perspective, these do not vary significantly from those raised by distributed software applications running on laptop computers outside the workplace. However, purchasing from on-line application (app) stores presents fresh risks.

11.3 Procedures

11.3.1 Baseline procedures

Responsibility	Procedure description
Management	***Certification of systems*** • Selection criteria for new systems must favour those systems which are already certified (see section 19, Assurance over security). ***Systems maintenance*** • Where an organisation lacks the internal resources to perform systems maintenance, this function must be contracted to an external party. ***Mobile applications*** • Scrutinise and assess the risks associated with the terms and conditions of the providers of mobile applications that are downloaded from App stores.
System administrator	***Apply security patches*** • As part of a regular maintenance cycle, apply software patches to application and systems software to manage, remove or reduce security weaknesses.

User (Developer)	***Preserve data integrity*** • Systems must have controls to ensure data input validation, checks on the loss of data integrity as a result of processing failures, message integrity and data output validation. ***Testing and test data*** • Test data must be selected carefully, protected and controlled. The use of operational data containing personally identifiable information (particularly patient NHI numbers), or any other confidential information, for developer-level testing purposes is not acceptable. • If such information is used for testing purposes (for example in user acceptance test environments which require substantial volumes of data that closely resemble operational data), all sensitive details and content must be protected. • System acceptance testing must include the testing of information security requirements. • Testing is to be performed in a realistic environment to ensure a system will not introduce vulnerabilities to the organisation's environment and that the tests are reliable. ***Distributed and mobile applications*** • In addition to all standard or normal system design requirements, ensure all distributed and mobile applications are designed with the ability to tolerate communication failure. This includes off-line capabilities and duplicate or out-of-sequence response message handling.

11.3.2 Intermediate procedures

Responsibility	Procedure description
Management	***Certification of systems*** • Security requirements must be identified and agreed prior to the development, acquisition and/or implementation of information systems. • Promote the use of cryptography controls to achieve information security where appropriate.
System administrator	No additional requirements in this section
User (Developer)	***Cryptographic keys*** • Where cryptographic controls are used, keys must be protected against modification, loss, destruction and unauthorised disclosure. ***Preserve data integrity*** • Systems must support data integrity audits where messages are traceable and reportable.

	Testing and test data • The access control procedures, which apply to operational application systems, must also be applied to test application systems.

11.3.3 Advanced procedures

Responsibility	Procedure description
Management	***Certification of systems*** • Mandate the use of cryptography controls to assist in achieving greater information security.
System administrator	No additional requirements in this section
User (Developer)	***Identify potential security vulnerabilities*** • Regularly check reliable sources of information about technical vulnerabilities. ***Preserve data integrity*** • Operating system services must be locked down to minimise the risk of vulnerabilities and intrusions. ***Software development*** • Industry best practices must be followed in all software development projects (whether internal, out-sourced or purchased products) for the capture, display, processing, exchange and persistence of sensitive information. In particular: o the use of established code libraries, algorithms and routines to implement security features and counter known threats o source code control o technical reviews o testing – unit, integration, compliance and user acceptance o documentation – for user, business and technical audiences o change control and version management o deployment mechanisms. ***Testing and test data*** • Separate authorisation is required each time operational information is copied to a test environment. • Operational information must be erased from a test environment immediately after the testing is complete. The copying and use of operational information must be logged to provide an audit trail.

12 Incident management

12.1 Objective

Ensure the appropriate tools, processes and procedures are in place to detect, report and manage information security incidents.

A health information security incident may be either a security breach or malfunction. A potential security incident may also be a threat or weakness that has been identified, which may have a detrimental impact upon the business.

12.2 Policy requirements

While specific policies are not required, procedures to ensure incidents are managed accordingly when they occur are addressed below.

The Protective Security Requirements (PSR), and the New Zealand Information Security Manual (NZISM) have very specific incident management requirements. The following is an extract from the PSR that lists the high-level controls required.

Security incidents	• Examples of security incidents • Roles and responsibilities in security incident reporting.
Reporting security incidents	• Reporting security weaknesses • Learning from incidents • Disciplinary process • Procedures for ensuring staff report recorded security incidents • Recording incidents • Dealing with minor security incidents • Dealing with major security incidents.
Investigations	• Principles of procedural fairness • Types of investigations • Agency procedures for investigating security incidents • Understand the role of an investigator • Determine the nature of an investigation • Terms of reference for investigations • Conducting investigations.

12.3 Procedures

12.3.1 Baseline procedures

Responsibility	Procedure description
Management	***Incident procedures*** • Establish management responsibilities to ensure procedures for incident management are developed and communicated within the organisation/applicable external parties. • Create and maintain procedures for incident logging, response, handling, escalation and recovery. ***Incident notification*** • Ensure all employees and contractors are aware of their responsibilities around reporting information security incidents/events/weaknesses, including who to report to and the location of the applicable policies/procedures. • Notify vendors and/or certifying bodies of failures in system security controls. • Notify other agencies/departments running similar technologies or who may be at risk to the same threat, if an incident occurs. • Notify all affected parties of the security incident and possible consequences eg, loss of data integrity. • Report significant information security incidents to the National Cyber Security Centre - www.ncsc.govt.nz/incidents. ***Incident response*** • Respond to reported security events and weaknesses in a quick, effective and orderly manner. • Facilitate protection and collection of evidence related to a security event involving staff disciplinary or legal action. • Develop a policy to handle duress situations.
System administrator	***Protect*** • Implement and maintain toolsets that can detect/defend against malware and viruses. • Ensure tools cannot be disabled by users. ***Monitoring and alerting*** • Log, alert and monitor systems/logs for significant events indicating health information security breaches and weaknesses. ***Report events*** • Educate users, contractors and third parties in how to report security incidents. • Report any weaknesses identified and security events as they occur. • Follow instructions from management for recording and monitoring security incidents.

	Incident response • Implement business continuity plans if needed. • Record all information about an incident in the appropriate register. • Implement containment processes to ensure security incidents do not spread while they are being addressed. • Once all evidence is collected, use appropriate tools and procedures to restore the environment to a normal operating state.
User	***Report events*** • Report security events and weaknesses through appropriate channels as quickly as possible and in a confidential manner.

12.3.2 Intermediate procedures

Responsibility	Procedure description
Management	***Assess*** • Perform vulnerability assessments to determine where weaknesses may exist and improvements can be made. ***Incident monitoring*** • Develop formal event monitoring, reporting and escalation procedures to enable the types and volumes of incidents to be monitored. ***Continual improvement*** • Institute a process for continual learning and developing improvements from monitoring and analysis of security incidents. ***Procedures*** • Provide an anonymous mechanism for reporting suspected security issues so the person reporting can do so without fear of ramifications. ***Incident analysis*** • Develop a procedure to review any security incidents post event and provide recommendations for avoiding a similar incident in the future. • Implement improvements in process, tools or policies to reduce the likelihood of incident recurrence.
System administrator	***Protect*** Implement and maintain toolsets that can detect/defend against intrusion or data loss.
User	No additional requirements in this section

12.3.3 Advanced procedures

Responsibility	Procedure description
Management	***Tasks*** • Create and maintain procedures for the handling and storage of forensic incident evidence. ***Incident analysis*** • Review the information gained from security incidents to determine the cost of each incident. • Share the analysis with colleagues so everyone learns from incidents.
System Administrator	***Incident response*** The failure of critical and/or out-of-band patching is to be included in the incident response as an event.
User	No additional requirements in this section

13 Business continuity

13.1 Objective

Information security continuity must:

- be embedded in the organisation's business continuity management systems
- ensure availability of information processing facilities.

13.2 Policy requirements

Policy requirements include identification of:

- an acceptable loss of information security on health information and services
- an acceptable time frame for full recovery of information security
- procedures to recover and restore information security
- the triggers and threats which will cause the business continuity plan to be activated.

13.3 Procedures

13.3.1 Baseline procedures

Responsibility	Procedure description
Management	***Information security continuity established*** • Determine requirements for information security and the continuity of information security management in disruptive events. Capture these within the business continuity management process or within the disaster recovery management process. • Establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during a disruptive event. • Verify the established and implemented information security continuity controls at regular intervals to ensure they are valid and effective during disruptive events, ie, run a restore.
System administrator	No additional requirements in this section
User	No additional requirements in this section

13.3.2 Intermediate procedures

Responsibility	Procedure description

Management	***Information security continuity governance***
	• An adequate management structure is in place to prepare for, mitigate and respond to a disruptive event using personnel with the necessary authority, experience and competence.
	• Incident response personnel with the necessary responsibility, authority and competence to manage an incident and maintain information security are nominated and appointed.
	Information security continuity planning
	Policies are to cover:
	• all information security aspects of both business continuity and disaster recovery programmes, for example: all related processes, procedures, supporting systems and tools
	• mechanisms to maintain existing information security controls in what may be highly adverse operating conditions
	• an ability to operate compensating controls within a known risk. management/mitigation process.
	Information security continuity plan verification
	Organisations must verify their information security management continuity by:
	• regularly exercising and testing the:
	  ○ functionality of information security continuity processes, procedures and controls to ensure they are consistent with the information security continuity objectives
	  ○ knowledge and routine required to operate information security continuity processes, procedures and controls to ensure their performance is consistent with the information security continuity objectives.
	• reviewing the validity and effectiveness of information security continuity measures when information systems, information security processes, procedures and controls or business continuity management/disaster recovery management processes and solutions change.

System administrator	***Availability of information processing facilities*** • Information processing facilities must be implemented with redundancy sufficient to meet organisational availability requirements. • Information restores are tested regularly.
User	No additional requirements in this section

13.3.3 Advanced procedures

Responsibility	Procedure description
Management	***Availability of information processing facilities*** • Organisations must identify business requirements for the availability of information systems. Where the availability cannot be guaranteed using the existing systems architecture, redundant components or architectures must be considered. • Where applicable, redundant information systems must be tested regularly to ensure the failover from one component to another component works as intended.
System administrator	No additional requirements in this section
User	No additional requirements in this section

14 Compliance

14.1 Objective

Avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and/or security requirements.

14.2 Policy requirements

The organisation's approach to meeting these requirements must be explicitly identified, documented and kept up to date for each information system and the organisation. The major regulatory requirements to be considered are listed above – see New Zealand legislation. Important relevant codes and guidelines are listed in Appendix D – Related specifications

14.3 Procedures

14.3.1 Baseline procedures

Responsibility	Procedure description
Management	• Identify and document all relevant legislative statutory, regulatory, and contractual requirements, and the organisation's approach to meeting these requirements. Regularly update documentation for each information system and for the organisation. In particular establish procedures to ensure: ○ compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products ○ records are protected from loss, destruction, falsification, unauthorised access and unauthorised release, in accordance with legislative, regulatory, contractual and business requirements ○ privacy and protection of personally identifiable information as required in relevant legislation and regulation. • Perform regular reviews for the compliance of information processing and procedures relating to the security policies, standards and any other security requirements. • Perform a risk assessment for all information systems at least every two years, or in accordance with section 19 Assurance over security, or if required following significant business or technology changes to systems, contract renewals, extensions and/or vendor changes.
System administrator	• Perform regular reviews of information system security operating procedures and practices as directed. • Undertake regular security-related testing activities as directed or stated in system certification & accreditation documentation, including but not limited to penetration (vulnerability) testing and disaster recovery testing.
User	Report areas of non-compliance to management.

14.3.2 Intermediate procedures

Responsibility	Procedure description
Management	• Take legal advice on legislative requirements as necessary. • Perform risk assessments for all new and changed systems.
System administrator	Undertake technical compliance review.
User	No additional requirements in this section

14.3.3 Advanced procedures

Responsibility	Procedure description
Management	• Risk assessments applied to all projects/business cases requiring IT Board approval • Determine the Cryptography and cryptographic key management (section 15) required to comply with relevant agreements, legislation and regulations • Undertake an independent review of the organisation's approach to managing information security and its implementation (ie, control objectives, controls, policies, processes and procedures for information security) at planned intervals or when significant changes occur • Conduct and report on organisational ICT assurance processes regarding security matters (eg, incidents, responses, issues, risks). This may include undertaking specialist internal/external audits of ICT environments and taking appropriate action based on findings and recommendations.
System administrator	Implement ICT security and privacy controls as required by business requirements (eg, see NZISM).
User	No additional requirements in this section

15 Cryptography and cryptographic key management

15.1 Objective

Ensure the proper and effective use of cryptography to protect the confidentiality, authenticity, integrity and/or availability of information using approved cryptographic products, algorithms and protocols.

Encrypt sensitive information to secure it from outside and insider threats.

15.2 Policy requirements

Cryptographic controls and keys must be protected by policies and procedures that ensure they are implemented, continue to be used, and are decommissioned in a manner that reduces the risks of unauthorised access and misuse. Such policies and procedures should exist at different levels across a chain of suppliers, vendors, suppliers, software developers and organisations using cryptographic products.

Note: Cryptography is a specialist area of information technology.
Organisations must seek specialist advice on selecting the appropriate cryptographic controls to meet their information security policy requirements.

Standard requirements for encryption technologies and algorithms are provided in the (NZISM) – see Appendix D – Related specifications

As part of developing a policy for the use of cryptographic controls, consideration should be given to the selection of appropriate encryption controls. The implementers of the policy should be able to answer the following questions.

- When do I use transport-level encryption vs application level for information in transit?
- When do I use a VPN or micro VPN connection for application-to data connectivity?
- When I encrypt data at rest, do I do this via the application, via database technology (where appropriate) or via infrastructure (particularly for cloud storage services)?
- Am I using/considering the most current encryption protocols and/or standards in the solution (with a view to minimising/addressing all known vulnerabilities pertinent to protection of the system information)?

15.3 Procedures

15.3.1 Baseline procedures

Responsibility	Procedure description
Management	***Procurement of cryptography*** When making new purchases (software, hardware, cloud services etc) use that time as an opportunity to have vendors and suppliers prove to you their cryptographic products are secure, in that they: • treat equipment to be returned to the supplier for repair, upgrade etc in a manner that protects any patient identifiable information that may still be on it • provide an alert at least 30 days before the expiry of cryptographic keys, to allow adequate time for arrangements to be put in place for their renewal.
System administrator	• Join user groups for the products using cryptographic controls and sign up to automatic notifications and alerts. • Keep systems patched and up to date, and give priority to critical notifications. • Manage the distribution and revocation of end-user and system certificates, with a minimum of delay. • Set a minimum notification period of 30 days for the renewal of any external certificate(s). • Ensure encryption is enabled on all equipment that is dependent on its own controls to protect itself, such as mobile devices, backups, and offsite storage. • Where tick box options are available, configure equipment to enable Federal Information Processing Standards (FIPS) compliance, sometimes referred to as 'FIPS mode' unless backwards compatibility to non-FIPS compliant systems is required (NZISM V2.3 May 2015 section 17.2.11). • Seek approval for disabling encryption when required for investigative purposes, and reinstate encryption when that work is completed.
User	• Do not share passwords and/or access relating to cryptographic keys with unauthorised persons. • Report lost and stolen equipment to IT support for appropriate actions to be taken. This action may include remotely wiping or disabling the device. • Comply with any notification requirements from IT support. • change your user passwords when equipment has been returned to you after repair. • Ask to be briefed on encryption and key management arrangements.

15.3.2 Intermediate procedures

Responsibility	Procedure description
Management	People with accountability for cryptographic systems ensure: • security expectations for cryptography and key management are communicated for both new projects and ongoing service delivery • responsibilities are clear and unambiguous for cryptographic systems and key management. This includes responsibility for planning security services that provide oversight for cryptographic systems for the outyears • exemptions (for non-compliance) and breaches are reported to corporate governance bodies, for systems managed both internally and outsourced • exercises for and updates to risk management, incident response and security practices take place on at least an annual basis. This may include table-top exercises and reviews or audits • contracts comply with cryptographic and key management guidance by preferring solutions that will be upgradeable for the foreseeable system lifetime over one-off point-solutions • changes to residual risk are detected, especially for technology challenges and threats that may influence ongoing accreditation • non-compliance procedures (written exemptions etc) are invoked only for the short term to allow for maintenance and upgrades that will bring systems back into compliance • recognise that transition periods where legacy cryptography and replacement solutions running side-by-side represent potentially a higher risk than running either solution alone • residual security risks are taken into account when accrediting these systems • equipment used to generate, store and archive keys is physically protected • relevant training and awareness programs are made available for administrators and users.
System administrator	• Reduce susceptibility to downgrade attacks by removing weak security solutions from selection. Likewise, clear text should only be able to be selected for diagnostic purposes and not operational periods where live data requires protection. Systems are returned to a secure state after running diagnostics. • Implement logging and auditing of key management related activities. • Frequently test the backup and restoration to and from removable media to ensure it can meet business needs. • Provide assurance to executive management that cryptographic systems continue to function as intended and that risks continue to be managed and minimised. This may include risk assessments and planning security services for IT systems for the outyears. • Treat systems used for generating and storing cryptographic keys according to the principles of a higher security classification, as those systems represent potential access to aggregated information and if compromised could undermine the separation of duties.

	• Lost and then found equipment, where it has been outside of a user's or an organisation's possession should be treated with suspicion. Such devices should be reloaded with fresh keys and passwords and the old keys revoked. • Carryover of keys to new equipment is discouraged between legacy to replacement systems, or old hosting providers to new, to reduce the transfer of old risks into new systems. • Options for the recovery of encrypted information are considered in contracts, particularly if the data is stored only in one place such as a hosting provider that could suddenly go out of business, or an end user device that could be lost or compromised. • Encryption of stored and transmitted information is facilitated by the use of cryptographic controls in a manner that represents a separation of duty and minimises any single point of failure or single point of compromise.
User	• Ensure familiarity with the organisation's policy on the usage of cryptography controls. • Seek advice from IT support when procuring new technology.

15.3.3 Advanced procedures

Responsibility	Procedure description
Management	***Establish and document a cryptographic policy*** • Adapt then adopt the requirements of the Protective Security Requirements and the *New Zealand Information Security Manual* as a security baseline for cryptographic controls and key management. • Define how the standards will be implemented throughout the organisation. • Categorise the information needing to be protected and assign the relevant encryption standards. • New cryptographic products and services are to be evaluated during procurement to ensure their cryptographic protocols, algorithms, key strengths etc. are upgradable over the expected lifetime of the system(s) proposed. This is in response to a changing threat environment, exploitable vulnerabilities being discovered, and as a protection against unintended misconfiguration. • Non-upgradable cryptographic solutions are avoided, except for short-lifetime disposable technologies (devices) that can be quickly decommissioned and replaced in response to an event or incident. • Cryptographic key lifetime (eg, validity start date, validity end date, and validity period) is appropriate and key materials are fit for the renewal cycle. Keys should not normally have a validity period of more than two to three years. • Weak cryptographic capabilities when tolerated in legacy systems (supported by time-bound written exemptions etc), are improved at the next upgrade. • Development, test and production environments have separate chains of trust to support a separation of duties. • Revoke then replace compromised cryptographic controls (protocols, algorithms and keys) in a timely manner when responding to a security event or incident.
System administrator	• Reduce susceptibility to downgrade attacks by ensuring revoked and or weak solutions are not reintroduced as a result of patching and upgrades • be familiar with conceptual guidance for key management, such as the PKI chapter of https://www.cs.auckland.ac.nz/~pgut001/pubs/book.pdf **Note:** you will need to copy this reference into a browser and access the document from there.
User	No additional requirements in this section

16 Suppliers

16.1 Objective

Have policies and procedures in place to protect health information exposed to third party organisations involved throughout a supply chain process agreed upon within contractual agreements.

This section must be read in conjunction with Section 11 System acquisition, development and maintenance

16.2 Policy requirements

The review and auditing of services against contractual agreements by external suppliers must be informed by the following policies.

- Define and document the criteria for selecting a supplier
- Assess supplier risks
- Create a formal contract and confidentiality agreement
- Establish access controls appropriate to the degree of risk identified
- Monitor compliance with all contractual terms
- Ensure that all information assets are returned and all access rights revoked, on the termination of agreements
- Ensure suppliers and government information is appropriately protected (MBIE Government Rules of Sourcing – Rule 5 : Types of supplier lists).

16.3 Procedures

16.3.1 Baseline procedures

Responsibility	Procedure description
Management	***Designated business process owner*** ***Supplier relationships*** • Assess and manage business, commercial, financial and legal risk associated with suppliers. • Approve potential suppliers based on risk profile. • Determine the frequency of audits. • Mandate security controls to manage risks. • Appoint legal representation to oversee contracts and agreements. • Assign responsibility for managing supplier relationships to an individual (eg, contracts or commercial manager). ***Supplier agreements*** • Establish and document supplier agreements to clarify the responsibilities of all parties involved in regarding fulfilling information security requirements. • Create appropriate formal service level agreements or equivalent with penalty clauses. • Check implementation of agreements with third-party suppliers, monitor their compliance with health information security requirements and manage changes to ensure security controls are operated and maintained properly.
System administrator	***Designated system process owner*** ***Supplier relationships*** • Assess and manage technical security risks associated with suppliers. ***Supplier agreements*** • Document incidents where requirements are not met. • Escalate incident reports to administrators and management.
User	***Supplier relationships*** • Implement controls for the monitoring and auditing of information access. ***Supplier agreements*** • Implement controls for monitoring the exchange of information between various parties to ensure agreed requirements are met and any risks that were not covered in the original agreement are highlighted. ***Store audit trail of system access*** • Store audit trail of data changes accessed by suppliers.

16.3.2 Intermediate procedures

Responsibility	Procedure description
Management	***Supplier relationships*** • Appoint owners for business processes requiring suppliers. • Create a standardised process and lifecycle for managing supplier relationships. • Assign responsibility for managing supplier relationships to an individual or service management team.
System administrator	***Supplier relationships*** • Work with information security, risk, supply/contract management and legal teams within the organisation as required.
User	***Supplier relationships*** • Define and document the types of information access different suppliers will require and be allowed to access. • Handle incidents and contingencies associated with supplier access. • Provide resilience, recovery and contingency arrangements to ensure the availability of information for processing. ***Supplier agreements*** • Implement controls for monitoring the exchange of information between various parties to ensure the requirements in the agreement are met and to highlight any risks not covered in the original agreement. ***Store audit trail of system access*** • Operate and maintain an audit trail of data changed by suppliers.

16.3.3 Advanced procedures

Responsibility	Procedure description
Management	***Supplier relationships*** Provide awareness training for personnel interacting with suppliers.
System administrator	No additional requirements in this section
User	No additional requirements in this section

17 Mobile devices and working outside the office

17.1 Objective

To ensure the security of the organisation's information and assets when employees are working outside the office, using mobile devices or when non organisation devices are used to access the organisation's information.

17.2 Policy requirements

17.2.1 Mobile devices (owned & non-owned)

The use of mobile and non-organisation owned equipment for organisation business is a growing trend that must only be permitted following the development of clear and unambiguous conditions including rights over the information and images stored.

The mobile device policy must take into account the risks of the use of privately owned mobile devices or bring-your-own-device (BYOD). The policy and related security measures must also consider the following:

- Separation of private and business use of the devices, including using software to support such separation and protect business data on a private device (see NZISM, Section 21.1.20)
- Providing access to business information only after users have signed an end user agreement:
  - acknowledging their duties (physical protection, software updating, etc.)
  - waiving ownership of business data
  - allowing remote wiping of data by the organisation in the case of theft or loss of the device or when no longer authorised to use the service.
- Privacy legislation requirements.

Mobile devices must be physically protected. Specific procedures, taking into account legal, insurance and other security requirements of the organisation, must be established for cases of theft or loss of mobile devices. Most important is the protection of the health care information held on such devices.

17.2.2 Teleworking (working outside the office)

Teleworking refers to all forms of work outside of the office, including non-traditional work environments. This activity is commonly referred to as telecommuting, flexible workplace, remote work and virtual work environments.

A policy for organisations allowing teleworking activities must define the conditions for using teleworking.

17.3 Procedures

17.3.1 Baseline procedures

Responsibility	Procedure description
Management	• A policy and supporting security measures must be adopted to manage the risks introduced by using mobile devices. For example: the use of at least five digit passcodes on all mobile devices to gain access to the device. • Training must be arranged for personnel using mobile devices to raise their awareness of the additional risks resulting from this way of working and the controls implemented. • A policy and supporting security measures must be implemented to protect information accessed, processed or stored at teleworking sites. • Implement a BYOD policy that addresses the following issues: privacy, acceptable use, IT requirements, security requirements (applies to all devices and connections), service policy, ownership of applications on the device, ownership of data/information on the device user, requirements on the employee, lost and found procedures. • At least annually, review, update as needed and reissue/publish the policy document. Gain formal acknowledgement of changes from all users.
System administrator	• Implement information security controls for mobile devices in line with those adopted in the fixed use devices (laptops) to address threats raised by their usage out of the office. • Implement a process users must follow in the event of the loss of a device.
User	• Care is to be taken when using mobile devices in public places, meeting rooms and other unprotected areas. • Devices carrying important, sensitive or critical business information must not be left unattended and, where possible, must be physically secured.

17.3.2 Intermediate procedures

Responsibility	Procedure description

Management	• Institute a policy on the implementation of mobile device management (MDM) software for all mobile devices and those used out of office.
	• Do not allow the use of jailbroken devices.
	• Establish and operate an ability to:
	  ○ track devices
	  ○ use appropriate file storage products
	  ○ remotely wipe corporate information on devices in the case of theft or inappropriate use.
	• At least semi-annually, review, update as needed and reissue/publish the policy document. Gain formal acknowledgement of such changes from all users.

System administrator	• Enforce MDM policies that include configuration of the device, encryption of removable storage cards (SDcards in mobiles etc), passcode enforcement, detection of jailbroken devise. • Determine out-of-date operating systems and notify users to update. • Remotely wipe entire devices or selectively wipe corporate data as requested.
User	• Be aware that sometimes only data held in certain applications – such as email – can be wiped.

17.3.3 Advanced Procedures

Responsibility	Procedure description
Management	• Implement policy defining the applications that can be used for particular purposes. For example, the use of specialist applications for things such as medical picture taking, also support attachment of that picture to the clinical record. • At least quarterly, review, update as needed and reissue/publish the policy document. Gain formal acknowledgement of such changes from all users.
System administrator	• Enforcement of MDM policies. • Examine the potential for the use of micro VPN technologies where possible to prevent resident data on devices. • Secure applications for access and synchronisation of files rather than email being used as workaround.
User	No additional requirements in this section.

18 Cloud computing and outsourced processing

18.1 Objective

Health organisations should ensure security controls applied by cloud service providers to their information are appropriate, clearly specified and where appropriate, are built into contractual arrangements for that service. As a minimum they are to cover the following factors:

- transmission
- storage
- processing of information
- data centre infrastructure (such as physical access controls, third-party or sub providers credentials, building code compliance)
- encryption and decryption of data (where, when, how)
- recovery of client information and /or applications by the health organisation
- access to client information by third-parties (such as US Patriot Act, and other national jurisdiction laws).

Appendix C – Other information; Cloud computing background has supporting information regarding cloud computing in the context of this framework and relating to the seven policy areas below.

A clear understanding of the model adopted with its attendant risks, rights and obligations as specified in a cloud computing contract, forms an essential risk management tool to support the security of health information.

18.2 Policy requirements

Use a risk management approach to address at least the areas identified in the GCIO Cloud Computing Information Security and Privacy Considerations see Appendix D – Related specifications

The outcome of work in each section should form part of a formal application to the IT Board to use the selected cloud service provider where the cloud service to be provided is overseas.

Note: The health care organisation to ensure it is reviewing the current IT Board requirements for the use of cloud computing services – see National Health Information Governance Expert Advisory Group (HIGEAG), guidance on the use of cloud or hosted services managing health information.

Note: The IT Board does not maintain tools on the risk assessment of cloud service providers. While the IT Board provides some guidance, in general terms it defers to the AoG Cloud Guidance and tools to assist health organisations in relevant due diligence duties required below.

Note: All personally identifiable information outsourced to the cloud is to be considered and protected as **'MEDICAL – IN CONFIDENCE'**, unless assessed and classified otherwise. see PSR: Management of aggregated information.

A cloud sourcing policy must be formalised and identify the following criteria in addition to those stated elsewhere in this framework (such as confidentiality, integrity, availability):

- the classification, sensitivity and privacy factors of information to be stored, processed or transiting the cloud service
- the impact in New Zealand and on Government if information is unavailable
- the cloud organisation incident management, jurisdictional and contractual arrangements
- the third party provider (inter-) dependencies and capabilities

In all cases, while the GCIO maintains a register of risk assessments completed for cloud computing providers, the health organisation retains a responsibility to assess the provider (vendor/supplier) information and confirm:

- the GCIO registered risk assessments of the selected cloud computing provider is up to date
- the proposed provider is still compliant with IT Board requirements
- performance of reference checking of the provider to the best ability, notably through the questionnaire criteria on the GCIO All of Government Cloud Risk Assessment Tool
- if a privacy impact assessment report has been completed, it should include identifying how the cloud computing provider handles security/privacy breach complaints/queries, including host country jurisdictional privacy legal requirements.

18.3 Procedures

18.3.1 Baseline procedures

Responsibility	Procedure description
Management	***Risk assessment*** • Check whether the cloud service being considered is already registered with the IT Board or GCIO (to prevent duplication or unnecessary effort/cost). • Perform a security risk and assurance assessment on any cloud computing initiative as part of the organisation's cloud sourcing policy. ***Cloud sourcing policy*** • Establish or adopt and adapt the security aspects of an existing reputable cloud sourcing policy. • Select a provider that complies with the policy. ***Sovereignty*** • Document the considerations, assessment and method of addressing any identified sovereignty issues or risks relating to information security. ***Privacy*** • Consider undertaking privacy impact assessment if a current one does not exist covering the provider's service.

	Governance • Ensure the provider's service level agreement and usage terms are fit for purpose and in place in relation to information security. • Ensure the supplier service delivery assessment includes evidence around commercial integrity, resiliency, reliability and longevity as well as compliance to security practices. ***Confidentiality*** • Confirm the cloud computing organisation operates an appropriate (role based) identity access management system. • Confirm the cloud computing organisation protects New Zealand health information appropriately, such as the provision/enabling of NZISM approved encryption of data at rest and in transit. ***Integrity*** • Confirm agreed record destruction processes are in place. ***Availability*** • Confirm agreed record destruction processes are in place. ***Incident response/management*** • Confirm effective incident management and response processes for information security are in place.
System administrator	• On an ongoing basis and at least annually or on being put on (five working days formal/written) notice of pending or potential changes, evaluate and report compliance with aspects of the defined policy areas. • On an ongoing basis the system is to record and report significant variances in or changes to or within the operation of the policy areas.
User	On an ongoing basis report on unusual operational security aspects that affect the ability of the user to operate in the stated policy areas.

18.3.2 Intermediate procedures

Responsibility	Procedure description
Management	***Cloud sourcing policy*** • Select a provider who complies with the information security policy either by undertaking a formal request for proposal process or by choosing a provider from the GCIO register of cloud computing service providers. ***Sovereignty*** • Formally identify and assess the cloud computing organisation's head office and storage/processing site for information. This may include proposed back-up and replication sites/locations. • Review other legislation/regulation as well as the cloud computing organisation's access request processing protocols. ***Governance*** • Identify and formally assess the governance model as it relates to security applied by the selected organisation.

	Confidentiality • Identify and assess the confidentiality regime operated by the selected organisation. ***Integrity*** • Identify and assess the operating environment, employment procedures, and physical and systems security assertions made by the selected organisation. ***Availability*** • Identify and assess service level agreement availability specifications. ***Incident response/management*** • Identify and assess service level agreement incident specifications.
System administrator	• On an ongoing basis and at least quarterly or on being put on (seven days written) notice of pending or potential changes, evaluate and report compliance with the policy areas.
User	No additional requirements in this section.

18.3.3 Advanced procedures

Responsibility	Procedure description
Management	***Privacy*** • Identify and assess a locally prepared privacy impact assessment including reviewing ISO/IEC 27018:2014 for applicability of procedures described as protective of information privacy - see Appendix D – Related specifications •
System administrator	On an ongoing basis and at least monthly or on being put on (seven days written) notice of pending or potential changes, evaluate and report compliance with all aspects of the policy areas.
User	No additional requirements in this section

19 Assurance over security

19.1 Objective

Provide stakeholders, management and users with a degree of confidence that information and processes requiring protection have had their security scrutinised and have been found to be robust and clearly meet or exceed the security aspects of the Health Information Privacy Code. Where residual risks exist they are understood and accepted/managed.

Assurance over security is typically conducted and achieved in two steps: Security certification followed by accreditation (C&A). These are often undertaken as part of a two-to-three year planning cycle of work for all systems.

The NZISM (Section 4 "System Certification and Accreditation") provides a generic example that can be adapted then adopted for organisations that do not have an existing security assurance process.

Assurance over security does not mean that systems will be impenetrable to unauthorised users. It does mean that all reasonable measures have been taken to:

- identify the information that requires protection, scrutinise security and fix any defects
- clearly articulate and understand the residual security risks that remain within the health care organisation's tolerance for risk.

19.2 Policy requirements

Security certification is the first step. It provides a spot check and tests security controls to assess if a system can provide protection for the information and processes in a manner proportional to the harm that could result. Successful system certification delivers two products: the certification document and report, and a statement of residual security risks. If the system being assessed fails certification the reasons why should be made clear to the person(s) responsible for accreditation.

Accreditation is the second step. This provides the formal authority to operate a system in a production environment with live data. This is less formally referred to as approval to 'go live'.

Accreditation relies on a system having had its security controls tested and vulnerabilities and defects minimised in the security certification process. Residual security risks reported are to be understood and accepted as part of the accreditation process before issuing 'go live' approval. Unacceptable risks may require further work for the design and implementation of security controls, with a follow up assessment for effectiveness and risk reduction.

Certification and accreditation is not limited to information systems. It also apples to 'x-as-a-Service' providers, sites, buildings, rooms, and containers. Where the management of aggregated information is identified as a risk, decommissioning and destruction processes should also be assessed for inclusion.

A system may be reassessed where there are changes in threat levels against it or changes to the environment it is deployed to.

Regardless of the approach used, organisations must take into account the security aspects of the Health Information Privacy Code.

19.3 Procedures

19.3.1 Baseline procedures

Note: When decommissioning or reassigning equipment, simply deleting files or reinstalling/upgrading a device is not effective at stopping data from being retrieved.

Responsibility	Procedure description
Management	***Security system certification*** • Communicate the business risks that the operational environment will be inheriting regardless of what technology is used to deliver a solution. • Identify privacy risks (often already identified in a privacy impact assessment). • Ensure that the physical security is appropriate. ***Accreditation*** • Understand the adequacy of the scope of testing and that appropriate actions were taken for the issues raised. • Understand and accept the system security certificate. • Understand and accept the residual risks. • Authorise a system to go into a live production environment with live data. ***Post accreditation*** • Prioritise patching for operating systems and application software. • Approve upgrades to operating systems and software applications.
System administrator	***Security system certification*** • Identify suitable existing common off-the-shelf products and services that meet the business need and already achieve security expectations. • Ensure testing demonstrates that security controls are effective and vulnerabilities and defects are minimised. • Advise management whether the testing conducted and reported demonstrated what it needs to, and if it can be relied on from a technical aspect. • Advise management of waivers/exemptions that may be required. ***Post accreditation*** • Patch and upgrade operating systems and application software.
User	***Acceptance testing*** • Ensure management is informed of the business process workflow and the associated risks.

19.3.2 Intermediate procedures

Responsibility	Procedure description

Management	***Accreditation***
	• Supply a profile for the information that requires protection. This may include the:
	  ○ criticality of the information
	  ○ other systems that rely on the system to be certified
	  ○ security classification of the data.
	• Communicate business continuity requirements and associated metrics.
	• State applicable standards (including sections within a standard that may otherwise not be applicable) and ensure all parties involved in the development and maintenance of systems are aware of their obligations.
	• Support security awareness, training and education requirements.
	Security system certification
	• Ensure information about the architecture and security controls is prepared before testing begins, so the testers know what they will be testing.
	Post accreditation
	• Approve the operating system and application software upgrades.

System administrator	***Security system certification*** • Ensure the assessment or report for compliance and effectiveness of the controls outlines areas of non-compliance and that any suggested remediation actions are made known to those responsible for Accreditation. ***Post accreditation*** • Advise management of changes over time to interfaces where testing may need to be re-performed and the results added to existing security certifications to keep them current. • Keep up to date with the latest advice for emerging risks and issues – (see Appendix C – Other information; Generic security information).
User	Participate in user acceptance testing and raise issues identified.

19.3.3 Advanced procedures

Responsibility	Procedure description
Management	***Security system certification*** • Identify risks associated with the management of aggregated information that may suggest large data collections should be treated according to the principles of a higher security classification. ***Accreditation*** • Ensure the security certification process is funded and promoted. • Establish a governance and management framework for the deliverables. • Support the planning and delivery of security assurance services for outyears to provide ongoing assurance that the system continues to provide the appropriate degree of protection during the certification period. • Where accreditation has expired, communicate outcomes to other agencies affected by the decision to accredit (or not). ***Post accreditation*** • Ensure technical documentation is being kept up to date. • Approve decommissioning procedures for superseded equipment. • Exercise incident management plans and processes (plan the exercise, exercise the plan).
System administrator	***Security system certification*** • Assist management to determine the security classification of the data and the aspects of managing aggregated information. • Translate business continuity requirements and associated metrics into 'IT Service Continuity' objectives. • Analyse the privacy impact assessment for any security considerations and advise management. • Draft statements of work for technical security services to be conducted. This should include: vulnerability assessments, penetration testing, identifying data transfer interfaces, and code review for bespoke software. • Assist with physical security assessments. ***Post accreditation*** • Keep technical documentation up to date. • Assess changes to decommissioning procedures. • Keep incident management plans and processes up to date.
User	No additional requirements.

Appendix A – Glossary

The table below defines the terms and acronyms used for the purposes of this framework.

Term	Definition
Assets	Data or images collected and stored (in a digital or hard copy format) and the information systems that are used to collect, store or exchange these data or images.
Authentication	Establishing that an agent using a computer system is the agent in whose name the account is registered.
Availability	Information is accessible and useable on demand by authorised entities.
Backup (noun)	The process of backing up refers to the copying and archiving of computer data so it may be used to restore the original after a data loss event. A backup and the associated procedures and processes can only be verified once the restore procedures and process have been confirmed via an actual restore.
Back up (verb)	To make a copy of data for the purpose of recovery.
Business Continuity Plan (BCP)	Documented procedures that guide organisations to respond, recover, resume and restore to a pre-defined level of operation following disruption.
Classification	Accords different levels of protection based on the expected damage, prejudice and/or loss the health information might cause in the wrong hands.
Cloud computing	Computer storage and processing power that is accessible over the internet and able to be connected to by anyone from either work, home or via mobile devices.
CMDB	Configuration Management Data Base.
Confidentiality	Information is not available or disclosed to unauthorised individuals, entities, or processes.
Cryptography	The science of coding and decoding messages so as to keep these messages secure. Coding (encryption) takes place using a key that ideally is known only by the sender and intended recipient of the message. Cryptographic control is the ability to render plain text unreadable and re-readable using cryptographic techniques. Such techniques are also used to ensure integrity and non-repudiation.
Custodian	In the health information security context a custodian is a person in an appointed role that is entrusted with the custody or care of a person's health information. An organisation may have custodianship over health care information.
Data elements	An indivisible piece of data, eg “first name”, “last name”, etc.
Data integrity	Data must not be altered or destroyed in an unauthorised manner and accuracy and consistency must be preserved regardless of changes.

Term	Definition
Disaster recovery (DR)	Disaster recovery is the process, policies and procedures related to preparing for recovery critical to an organisation after a natural or human-induced disruptive event. Disaster recovery planning is a subset of a larger process known as business continuity management (BCM). This includes planning for resumption of applications, data, hardware, communications (such as networking) and other IT infrastructure.
Disaster recovery plan (DRP)	A documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster.
Disruptive event	Any event, regardless of cause, that disrupts (or has the potential to disrupt) an organisation's ability to maintain identified critical functions.
Environmental (threats/hazards)	Threats or risks of physical harm. From an IT security viewpoint this is to do with physical access to or potential physical risks to hardware
Facility	A single physical location from which health goods and/or services are provided. A health care organisation may consist of multiple facilities. See also 'facility' as defined in HISO 10005/10006 Health Practitioner Index Standard
Firewall	A device or set of devices configured to permit, deny, encrypt or proxy all computer traffic between different security domains based upon a set of rules and other criteria.
GCIO	Government Chief Information Officer. A role operated out of the Department of Internal Affairs – see https://www.ict.govt.nz/governance-and-leadership/the-gcio-team/
GP	General practitioner.
GP2GP	The general practitioner to general practitioner patient notes transfer utility.
Health care (health care) provider	A person, facility or organisation providing patient health care services, including services to promote health, to protect health, to prevent disease or ill-health, treatment services, nursing services, rehabilitative services or diagnostic services. See practitioner.
HPI	Health Practitioner Index. The unique identifiers assigned to New Zealand health care providers, organisations and facilities.
ICT	Information and communications technology.
Interoperable Interoperability	The ability of products, systems, or business processes to work together to accomplish a common task. Systems share information and/or functionality with another system based upon common standards.
Malware	Software developed for malicious intent. This includes viruses, worms, adware, Trojan horses, keyloggers.
Media	Any technology used to place, keep, transport and or retrieve data. This includes both electronic devices and materials as well as non-electronic options eg, paper.
Medical-in-Confidence	An information security classification given to personal health information.

Term	Definition
NHI	National Health Index number. The number assigned to all individual health care consumers in New Zealand. see the Consumer Health Identity Standard – HISO 10046
NZISM	New Zealand Information Security Manual
Personal health information	Personal health information is health information identifiable to an individual.
Portable media	Media that can be used to transport electronic information independently of a network. This includes floppy disks, USB storage, portable hard-drives and other devices that have a data storage mechanism (cameras, cell phones, iPods etc.)
Practitioner	An individual who is engaged in a health care related occupation. See health care provider.
Privacy Impact Assessment (PIA)	An analysis of how an individual's or groups of individuals' personally identifiable information is collected, used, shared and maintained by an organisation.
Procedure	A specification or series of actions, acts or operations which have to be executed in the same manner in order to always obtain the same result in the same circumstances (eg emergency procedures).
Risk management	The identification, assessment, and prioritisation of risks including using resources to minimise, monitor, and control the impact of these risks.
Secure health network	A network connection between organisations or persons built and operated according to the technical specifications required to securely access or exchange personal health information.
Service level agreements (SLA)	A formally negotiated agreement between two parties that records the common understanding about services, priorities, responsibilities, guarantee, and such collectively, the level of service.
Software as a Service (SaaS)	The provision of a standardised application service – usually in a cloud or outsourced environment.
Systems	Applications or electronic business processes which support the collection, access, processing and exchange of personal health information
Teleworking	A work arrangement in which employees are able to have flexibility in their working location. That is: a central place of work is supplemented by a remote location (eg, home), usually with the aid of information technology and communications.
Treatment	The act of remediation of a health problem.
Virus	A computer programme that can copy itself and infect a computer without permission or knowledge of the user. Viruses usually corrupt or modify files on a targeted computer.
Worm	A self-replicating computer programme. It uses a network to copy itself to other nodes (computer terminals on the network) and it may do so without any user intervention. Worms almost always cause harm to the network, if only by consuming bandwidth, whereas viruses usually corrupt or modify files on a targeted computer.

Appendix B – Information classification principles

The purpose of an information classification system is to assign a security category to types of information, in either hard copy or electronic form, and to specify how the information and equipment that handles that information must be protected. It helps classify information based on a risk assessment of how much damage, loss or prejudice would result from compromising specific content. It limits access to information and equipment through a series of procedural and/or physical barriers.

Classifications for information that needs to be protected because of commercial and public interest or personal privacy are defined more fully in the Protective Security Requirements manual (Appendix D – Related specifications). The following are the principle categories that require particular protection for the health and disability sector:

- in confidence
- sensitive.

Information that requires protection is any information for which compromise threatens the security, safety or interests of individuals, groups, the commercial organisations, government business and the community.

Based on a generic risk assessment of how much loss, damage or prejudice would result from compromising specific content, the following classifications apply as a minimum:

Information	Classification
Personal health information	IN CONFIDENCE
Identifiable employee and practitioner information that is not intended for the public domain	IN CONFIDENCE
Commercially sensitive information that needs protection from unauthorised access	IN CONFIDENCE
Statistical information that is non–identifiable	Unclassified
All other information	Unclassified

Information that is classified IN CONFIDENCE or higher requires protection from unauthorised access during processing, transfer and while at rest. Endorsements must be used to differentiate Health, Staff and Commercial information types eg MEDICAL IN CONFIDENCE, STAFF IN CONFIDENCE and COMMERCIAL IN CONFIDENCE.

In addition, there is a category of IN CONFIDENCE information that requires special handling. The determination of the requirement for special handling is based on:

- organisational requirement. This can be legislation, policy or need based
- subject matter that is considered to require special handling eg, mental health information, sexual diseases, abuse, etc.

Information that requires special handling will use higher access standards for electronic solutions or an alternative manual process to ensure the 'need to know' principle is maintained. There may be occasional times when the information used in the health and disability sector must be classified at a higher level (aggregated information). It is the responsibility of the originator (a person or organisation) to complete that classification evaluation. See Protective Security Requirements

Where the aggregated amount of health information is considered to be significant, the collective Classification of that information set should be treated according to the principles of a higher classification.

Appendix C – Other information

Plan security services for the future

The following must be considered in building a risk profile.

- **Ongoing assurance for the outyears:** To assist business representatives to manage their risks and achieve their objectives, an approach "Planning security services for IT Systems". http://arxiv.org/abs/1409.5845 is an example that can be ***adapted then adopted*** where an organisation does not have a similar existing approach. This approach may be particularly helpful for new technologies such as cloud computing, mobile devices, or where devices on the edge of the network experience faster rates of technology advancement than at the core.

- **Upgradeable solutions:** Systems should be designed so their non-functional components, such as encryption protocols and algorithms can be easily upgraded via the patching process. One-off 'point solutions' that cannot be upgraded should be avoided in preference to solutions that will be upgradeable for the foreseeable system lifetime.

- **Decommissioning:** When exiting from an environment where there is little surety of encryption key materials not being compromised, advice in the NZISM for the management of key materials must be considered for its wider context.

Generic security information

The following additional references are provided for technical elements not fully covered by any of the above.

Generic security advice for New Zealanders and small to medium enterprises can be found at:

Netsafe	http://www.netsafe.org.nz/
ConnectSmart	http://www.connectsmart.govt.nz/
Cybersafety for SMEs	http://www.thewhatsit.org.nz
Cyberbullying information	http://www.cyberbullying.org.nz
Learn about computer security	http://www.netbasics.org.nz
National Cyber Security Centre Newsroom	http://www.ncsc.govt.nz/newsroom/

Cloud computing background

1. Cloud Computing models are defined in NIST-SP800-145. Additionally, ISO 17788:2014 and ISO 17789:2014 provide more technical detail for ICT staff (solution architects, system administrators, etc.) – see Appendix D – Related specifications.
2. Health organisations should ensure that the security controls that cloud service providers will apply to their information are appropriate, clearly specified, and where appropriate built into contractual arrangements. Such contractual arrangements could include compliance with controls as outlined in ISO 27000 series standards, notably ISO 27017 and ISO 27018. Ongoing evaluation of the established policies as well as adherence to those policies is equally fundamental.

3. This framework's cloud computing information security procedure categories are aligned to the cloud computing information security and privacy considerations (Appendix D – Related specifications):

a. Sovereignty

Identify, assess and evaluate:

- the location of both the head office of the cloud computing organisation and the site for information storage and processing (including proposed back-up sites/locations)
- relevant domestic and foreign legislation and regulations (particularly including privacy legislation)
- cloud computing organisation proposed responses to other government requests for access to information.

b. Privacy

The Office of the Privacy Commissioner is the primary compliance advisor for this framework and provides guidance for health care organisations in the application of the privacy law, privacy principles and use of the privacy impact assessment toolkit (see Appendix D – Related specifications). The GCIO cloud computing guidance includes both privacy and security in its questionnaire considerations.

c. Governance

Ensure the service providers service level agreement, terms of service, service descriptions or equivalent auditable documents incorporate service escalation processes, solutions and practical penalties; use of and access to clients data for any other purpose; proposals for the protection of client data (eg vulnerability scans, penetration testing); applicable industry and international standards (such as SOC2, ISO27001/2/17/18, etc.) or the service providers code of practice and its application; legal implications of the hosting jurisdiction, and intellectual property status etc.

d. Confidentiality

Assess and confirm the cloud computing organisation will operate an appropriate identity access management system and, if multi-tenancy is operating, review any related access rules.

Confirm the providers approach and responsibilities to maintaining the confidentiality (and availability) of client information; particularly the return or transfer of client information/data upon termination of the service, and complete removal of client information from the provider's systems.

e. Integrity

Identify and assess service level agreement or equivalent specifications as to:

- data/system/network availability for clearly defined period(s)
- fit with New Zealand business requirements
- business continuity planning, IT Service Continuity, backup and restore testing
- the inclusion of realistic disclosure of service level agreement breaches and penalties for non-compliance

- efficacy of proposed record destruction processes (eg during the termination of the contract for service provision).
  Note: particularly refer to the requirements of the New Zealand Public Records Act 2005 and the Official Information Act 1992.

f. Availability

Confirm data/system/network availability is for clearly defined agreed period(s) that fit with New Zealand business requirements.

g. Incident response/management

Confirm agreement has been reached covering:

- formal reporting of incident responses
- times to address the identification of high priority/impact faults
- recovery processes post incident including providing ongoing and timely advice of progress.

4. ISO 27017 provides guidance on the information security elements of cloud computing, recommending and assisting with the implementation of cloud-specific information security controls. This supplements the guidance in ISO/IEC 27002 and other ISO 27000 series standards including:
   - ISO/IEC 27018 on the privacy aspects of cloud computing
   - ISO/IEC 27031 on business continuity
   - ISO/IEC 27036-4 on relationship management.
5. ISO 27018 is a code of practice that ensures cloud service providers who are ISO 27018 certified offer suitable, contractually binding, information security controls and business practice commitments to protect the privacy of their customers' clients by securing personally identifiable information including personal health information entrusted to them.
6. Other self-certification and auditable standards exist that will address the majority of the categories and criteria raised in the Cloud computing and outsourced processing (Section 18). These include SOC1, 2, 3 (types 1 and 2), CSA STAR, CCM and CAIQ. Where cloud service providers support these applicable standards and assessment schemes, health organisations should include the cloud service provider certification with any cloud adoption proposal to the IT Board about use of the cloud services.

Appendix D – Related specifications

The documents listed below have been used or referred to in the development of this standard. They may provide some further clarity, if required.

Aiming for Excellence - The Royal New Zealand College of General Practitioners' standard for general practice https://www.rnzcgp.org.nz/quality-standards

All-of-Government - Requirements for Cloud Computing: https://www.ict.govt.nz/guidance-and-resources/information-management/requirements-for-cloud-computing

All-of-Government Information Security Risk Assessment Framework: https://www.ict.govt.nz/guidance-and-resources/information-management/privacy-and-security/

All-of-Government ICT Operations Framework https://www.ict.govt.nz/ict-system-assurance/about-ict-system-assurance/ict-assurance-frameworks/

All-of-Government ICT Security and Related Services Panel: https://www.ict.govt.nz/services/show/SRS-Panel

AS/NZS 27001/2:2013 *Information Security Management*.

AS/NZS ISO/IEC 27002 - *Information technology - Security techniques - Code of practice for information security management* [4]

Note: The Ministry of Health has a copyright licence to use part of this publication in the present document. However, if organisations wish to purchase the referenced document, copies can be obtained from www.standards.co.nz.

Cloud Computing Requirements and Guidance (Government Chief Information Officer (GCIO)): https://ict.govt.nz/guidance-and-resources/information-management/requirements-for-cloud-computing

Cloud Computing Information Security and Privacy Considerations (GCIO Publication): http://www.ict.govt.nz/assets/ICT-System-Assurance/Cloud-Computing-Information-Security-and-Privacy-Considerations-FINAL2.pdf

Code of Health and Disability Services Consumers Rights: http://www.hdc.org.nz/the-act--code/the-code-of-rights

Connected Health Network Connectivity Standards - HISO 10037: http://healthitboard.health.govt.nz/hiso-10037-connected-health-network-connectivity-standards

Consumer Health Identity Standard - HISO 10046: http://healthitboard.health.govt.nz/hiso-10046-consumer-health-identity-standard

Evidence of Identity Standard Version 2, December 2009, Department of Internal Affairs: http://www.dia.govt.nz/Resource-material-Evidence-of-Identity-Standard-Index

Federal Information Processing Standards (FIPS) http://csrc.nist.gov/publications/PubsFIPS.html

Government Enterprise Architecture NZ (GEA-NZ) Standards: https://www.ict.govt.nz/guidance-and-resources/standards-compliance

Guidance to offshore ICT providers: http://ict.govt.nz/guidance-and-resources/agency-guides/government-use-offshore-ict-service-providers

Health Information Privacy Code 1994 (HIPC) and amendments https://www.privacy.org.nz/the-privacy-act-and-codes/codes-of-practice/health-information-privacy-code

[4] This document was originally numbered AS/NZS ISO/IEC 17799:2006

Health Practitioners Competence Assurance Act 2003
http://www.legislation.govt.nz/act/public/2003/0048/latest/DLM203312.html

Information Technology Infrastructure Library (ITIL):
http://www.itil.org.uk/.

ISO/IEC 11179 *Information Technology – specification and standardization of data elements. Part 3: Basic attributes of data elements*, Second edition 2004

ISO/IEC 17788:2014 Information Technology – Cloud Computing – Overview and vocabulary

ISO/IEC 17789:2014 Information Technology – Cloud Computing - Reference Architecture

ISO/IEC 27018:2014 Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

ISO/IEC 27799:2008 Health informatics -- Information security management in health using ISO/IEC 27002

ISO 31000 Risk Management:
http://www.iso.org/iso/home/standards/iso31000.htm

MBIE Government Rules of Sourcing:
http://www.business.govt.nz/procurement/for-agencies/key-guidance-for-agencies/the-new-government-rules-of-sourcing

National Health IT Board – Use of Cloud services
http://healthitboard.health.govt.nz/standards/use-cloud-or-hosted-services-managing-health-information

National Health IT Plan, published September 2010, Ministry of Health:
http://www.ithealthboard.health.nz/content/national-health-it-plan

National Health Information Governance Expert Advisory Group (HIGEAG), Use of Cloud or hosted services managing health information:
http://healthitboard.health.govt.nz/standards/use-cloud-computing-managing-health-information

New Zealand Information Security Manual (NZISM) version 2.3 May 2015
http://www.gcsb.govt.nz/news/the-nz-information-security-manual

The NIST Definition of Cloud Computing:
http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Office of the Privacy Commissioner (OPC) Cloud Computing a Guide to Making the Right Choices - February 2013:
http://privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/OPC-Cloud-Computing-guidance-February2013.pdf

Office of the Privacy Commissioner (OPC) Privacy Impact Assessment Handbook – June 2007:
http://privacy.org.nz/assets/Uploads/Privacy-Impact-Assessment-Handbook-June2007.pdf

Operational Policy Framework (OPF):
http://nsfl.health.govt.nz/

Privacy at work, a guide to the Privacy Act for employers and employees:
https://www.privacy.org.nz/news-and-publications/books-and-articles/privacy-at-work-a-guide-to-the-privacy-act-for-employers-and-employees/

Protective Security Requirements (PSR):
http://www.protectivesecurity.govt.nz/home/protective-security-governance-requirements/

http://www.protectivesecurity.govt.nz/home/protective-security-governance-requirements/reporting-incidents-and-conducting-security-investigations/

https://protectivesecurity.govt.nz/home/information-security-management-protocol/management-of-aggregated-information/