

Health Information Security Framework Essentials and Recommendations

HISO 10029.1

To be used in conjunction with
HISO 10029.2 Health Information Security Framework
Templates and Samples

Copyright Information

This document has been approved as a standard for the New Zealand health and disability sector by HISO.

The copyright owner of this document is the Ministry of Health, which is part of the New Zealand Crown. This document may be reproduced, in whole or part, in any number of copies and in any format or medium provided:

- the content is not changed
- the material is not sold
- the material is not used to promote or endorse any product or service
- the material is not used in an inappropriate or a misleading context having regard to the nature of the material
- any disclaimers included on the published information are reproduced on the material
- a copyright acknowledgment to the New Zealand Ministry of Health is included.

Any reproduction of the document must respect the moral rights of the author of the work as set out in Part IV of the Copyright Act 1994.

Party other than the Ministry of Health

Permission to reproduce Ministry of Health work does not extend to include any work identified in this document as the copyright material of a party other than the Ministry of Health. Authorisation to reproduce such material must be obtained from the copyright holders concerned.

Copyright enquiries

If you are in doubt as to whether a proposed use is covered by this license, please consult the Web and Publications Manager of the Ministry of Health.

Published in August 2009, by the Ministry of Health
PO Box 5013, Wellington, New Zealand

ISBN 978-0-478-31876-0 (online)

**This document is currently available on the HISO website:
<http://www.hiso.govt.nz>**

Contents

1	Foreword	1
2	Introduction	3
2.1	Documents.....	3
2.2	Background.....	3
2.3	Scope.....	4
2.4	Security Controls	5
3	Governance and Management Requirements	7
3.1	Governance	8
3.2	Accreditation and Certification	9
4	Structure of the Policies	10
4.1	Section layout	10
5	Information Security Policy.....	11
5.1	Objective	11
5.2	Policy Statements	11
5.3	Procedures.....	11
5.4	Guidelines for Small Organisations	11
5.5	Checklist for Compliance	11
6	Organising Information Security.....	12
6.1	Objective	12
6.2	Policy Statements	12
6.3	Procedures.....	12
6.4	Guidelines for Small Organisations	13
6.5	Agreements for Third Party Access	13
6.6	Checklist for Compliance	14
7	Asset Management	15
7.1	Objective	15
7.2	Policy Statements	15
7.3	Procedures.....	15
7.4	Guidelines for Small Organisations	16
7.5	Guidelines for Retention/Disposal of Health Information.....	16
7.6	Checklist for Compliance	17
8	Human Resources Security	18
8.1	Objective	18
8.2	Policy Statements	18
8.3	Procedures.....	19
8.4	Guidelines for Small Organisations	20
8.5	Checklist for Compliance	20
9	Physical and Environmental Security.....	21
9.1	Objective	21
9.2	Policy Statements	21
9.3	Procedures.....	21
9.4	Guidelines for Small Organisations	22
9.5	Checklist for Compliance	22
10	Communications and Operations Management Policy	23
10.1	Objective.....	23
10.2	Policy Statements.....	23
10.3	Procedures	24
10.4	Guidelines for Small Organisations	25
10.5	Checklist for Compliance.....	25
11	Access Control.....	27
11.1	Objective.....	27

11.2	Policy Statements	27
11.3	Procedures	27
11.4	Guidelines for Small Organisations	29
11.5	Checklist for Compliance	30
12	Information Systems Acquisition, Development and Maintenance	31
12.1	Objective	31
12.2	Policy Statements	31
12.3	Procedures	31
12.4	Guidelines for Small Organisations	32
12.5	Checklist for Compliance	32
13	Incident Management	33
13.1	Objective	33
13.2	Policy Statements	33
13.3	Procedures	34
13.4	Guidelines for Small Organisations	34
13.5	Checklist for Compliance	35
14	Business Continuity	36
14.1	Objective	36
14.2	Policy Statements	36
14.3	Procedures	36
14.4	Guidelines for Small Organisations	36
14.5	Checklist for Compliance	37
15	Compliance	38
15.1	Objective	38
15.2	Policy Statements	38
15.3	Procedures	39
15.4	Guidelines for Small Organisations	39
15.5	Checklist for Compliance	39
Appendix A – Glossary		40
Appendix B – Information Classification Principles		44
Appendix C – Media Risk Assessment		45

Tables and Figures

Table 1: Security Control Section Headings	6
Table 2: Procedures for Information Security Policy.....	11
Table 3: Procedures for Organising Information Security	13
Table 4: Procedures for Asset Management	16
Table 5: Procedures for Human Resources Security	19
Table 6: Procedures for Physical and Environment Security.....	22
Table 7: Procedures for Communications and Operating Management Security	25
Table 8: Procedures for Access Control	29
Table 9: Procedures for Information Systems Acquisition, Development and Maintenance.....	31
Table 10: Procedures for Incident Management.....	34
Table 11: Procedures for Business Continuity.....	36
Table 12: Procedures for Compliance	39
Table 13: Information Classifications	44
Table 14: Media Risk Assessment.....	46
Figure 1: Health Information Security Framework	7

Committee representation

Committee 10029 was responsible for the preparation of this document. It comprised representatives of the following nominating organisations:

Nominating Organisation	Representative
Health Alliance	Dr Ross Boswell
Healthlink Ltd	Tom Bowden
Hutt Valley District Health Board	Tony Cooke
Consumer representative	Jo Fitzpatrick
New Zealand Nurses Organisation	Cathy Gilmore
Genesis Consulting Group Limited	Shayne Hunter
PCIMG/Massey University	Dr Inga Hunter
National Institute for Health Innovation	Dr Lech Janczewski
RNZCGP	Dr Anthony Kriechbaum
Pharmacy Guild of New Zealand	Alex Lees
Elisabeth Harding and Associates	Graeme Miller
Health Alliance	Dr Martin Orr
Auckland University of Technology	Dr Dave Parry
Health Intelligence	Tony Randle
Ministry of Health	Peter Aagaard
Telecom	Malcolm Shore
IBA Health (NZ) Ltd	Graham Starkey
State Services Commission	Chris Steenkamp
TelstraClear	Neil Stevenson
State Services Commission	Colin Wallis
IPAC	Chris Walmsley
Faculty of Law, University of Otago	Richman Wee

Related documents

The documents below have been used in the development of this framework. They provide further clarity if required.

Standards New Zealand

SNZ HB 8169:2002 Health Network Code of Practice

Standards Australia

HB 174-2003 Information Security management – Implementation Guide for the Health Sector

ISO

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

Other publications

Health Information Privacy Code 1994

Code of Health and Disability Services Consumers Rights

New Zealand legislation

The Privacy Act 1993

www.security.govt.nz/sigs/ (Security in the Government Sector)

www.e.govt.nz/standards/e-gif (Government Interoperability Framework Standards)

www.gcsb.govt.nz/

<http://www.e.govt.nz/policy/trust-security/offshore-ICT> (guidance to offshore ICT providers)

Referenced Documents

The documents below have used for reference throughout this framework.

AS/NZS

AS/NZS ISO/IEC 27002:2006 (renamed from 17799:2006) - Information technology - Security techniques - Code of practice for information security management ¹

HISAC (Health Information Strategy Advisory Committee) has obtained a copyright licence to use part of this publication in this framework. However, if organisations wish to purchase the full document, copies can be purchased from www.standards.co.nz.

ISO/IEC

ISO/IEC 27001:2005 - Information technology - Security techniques-- Information security management systems – Requirements

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

If required, copies of these documents can be purchased from www.standards.co.nz

¹ This document was originally numbered AS/NZS ISO/IEC 17799:2006

1 Foreword

There were many challenges facing the HISO Expert Advisory Committee in developing a health information security framework. There was the large and diverse range of source material on security available to us. There was the need to clearly **classify** and define health information and to understand how privacy would fit into the framework.

The sheer quantity of source material about security, the different approaches on offer, the existing security codes of practice, the array of threats: technical, legal, and people-oriented, meant that we were faced with a wide range of choices in our approach. The problem was one of selection rather than creation of new material. After an initial assessment, we decided to adopt an international code of practice for security management, AS/NZS ISO/IEC 27002:2006. We believe the advantages of this code are that it is future-proof, will continue to develop independently and is already widely used by other organisations wanting to maintain good security practices.

We endeavoured to find the right balance of policies, procedures and technical controls to ensure an across-the-board improvement in the security of health information. Our mission was to lift the bar for every organisation and practitioner in New Zealand who holds health information. Known vulnerabilities and weaknesses in the current security framework needed to be addressed.

We wanted to design a health information security framework that was practical and understandable especially by the small health care businesses that make up the bulk of health and disability sector organisations. This meant pruning the available controls and alternatives to those which were absolutely essential and which every organisation from the sole practitioner to the large health care provider could follow. We also identified a number of *recommended* controls for organisations which either wish to follow best practice, which are of greater size, or which have a greater need to reduce their risk.

We have provided some “out of the box” tools for practitioners and organisations to use and adapt without having to undergo a detailed risk assessment of their own. This does not prevent an organisation from performing its own risk assessment, or from delving deeper into the methodology. In fact, the Committee advises that large organisations (>100 staff) use the AS/NZS ISO/IEC 27002:2006² methodology to develop their own organisational security policy, on the proviso that they do not contradict or undermine any of the essential policies outlined in this framework.

For the secure sharing of information, all organisations holding health information must follow common minimum standards of security so that the information can be passed on knowing that each party handles it with equal care.

The development of security for personal health information requires a balance between controls and accessibility. Too many security controls and the information becomes of no practical use, or is inaccessible to those who should have access to it. Furthermore, with controls comes the cost of compliance – too much cost and controls will inevitably be avoided. Conversely, a lack of security controls means that personal health information becomes devalued in the minds of users and confidence in health care can be easily eroded.

As members of the Expert Advisory Committee, we needed to find the right balance for the sector today. We did this by being prescriptive in some areas, while allowing a range of options in others.

The Health Information Security Framework the Committee has developed on behalf of the health and disability sector specifies the minimum policy standards and technical requirements to best enable organisations to safeguard patients’ health information.

A set of principles was used in the development of the framework. It

- is accessible to all parties in the sector
- provides practical guidance and samples (e.g. of policies)
- is tailored to the various sizes of organisations and audiences

² AS/NZS ISO/IEC 27002:2006 can be purchased from www.standards.co.nz

- covers a broad range of security areas
- is manageable, cost-effective and practical to implement
- provides governance, a support structure and compliance audits
- evolves over time with regular reviews

The Committee believes such a framework will be quickly taken up by the health and disability sector so the public can be confident their personal health information is maintained securely on their behalf.

Tony Cooke
Chair of HISO Expert Advisory Committee 10029

2 Introduction

2.1 Documents

The Health Information Security Framework comprises several documents. These are numbered as follows:

- 10029.1 Health Information Security Framework Essentials and Recommendations;
- 10029.2 Health Information Security Framework Templates and Samples;
- 10029.3 Technical Specifications Register (in development).

It is intended that these documents (or parts of documents) should be read together. They are separated here solely to simplify the structure of the standard, for ease of use.

2.2 Background

A sector-wide Health Information Security Framework is required to ensure that health information is produced, stored, disposed of and shared in a way that ensures the information's confidentiality, integrity and availability.

Confidentiality:	Information must not be made available or disclosed to unauthorised individuals, entities, or processes.
Integrity:	Data must not be altered or destroyed in an unauthorised manner and accuracy and consistency must be preserved regardless of changes.
Availability:	Information must be accessible and useable on demand by authorised entities.

The relationship of trust that exists between a patient and their health care practitioner is important for good health care. The health care practitioner is obligated to treat personal health information³ with proper care and respect and to keep it secure. If such information is disclosed inappropriately, corrupted or lost the consequences for both patient and practitioner are serious. Whilst personal health information is primarily used for delivering health care it is also, in the wider sense, an asset which is used for the purposes of supporting the business of health care, for teaching, research and for population health management. Without a consistent security standard applied to health information, patients cannot be sure that their information is kept confidential and secure.

A number of factors need to be considered when protecting personal health information. Computer systems have become pervasive in the collection, processing, transfer, storage, retrieval and disposal of health information. Technology can be both the cause of and the solution for security issues. With increasing specialisation and diagnostic testing, multiple practitioners are involved in patient care and personal health information is increasingly shared between organisations and/or practitioners. With such increasing use of technology and interconnectedness, personal health information is exposed to a wide variety of threats and vulnerabilities.

Some of these threats are, for example;

- Unauthorised use of a health information application through the user not logging out correctly, or leaving a workstation unattended in a location accessible to the public.
- Connection failures which can facilitate the disclosure of confidential information by forcing users to send information by a less secure medium, such as via fax or internet email.
- Introduction of damaging or disruptive software which can contain computer viruses and worms.
- Theft or loss of information assets through storage, without encryption, of health information on highly portable media such as laptops, CDs, DVDs, and USB devices.

³ Personal health information is health information identifiable to an individual

There is no one answer to keeping information secure and no set of controls that can achieve complete security. This framework aims to implement a broad range of measures to achieve “such safeguards that it is reasonable in the circumstances to take” as per Rule 5 of the Health Information Privacy Code.

2.3 Scope

Personal health information can exist in many forms. This framework is mainly concerned with the way information is held, transferred and retrieved using electronic health care systems. Wherever the same practices apply to paper records⁴ and other types of media, these are noted. Appendix C lists the different types of communication channels and assesses their relative risk, based on the risk of discovery in transmission or at the receiving end.

Our audience is all health organisations and organisations⁵ which hold personal health information. Our target audience is small organisations of less than 20 staff and medium sized organisations of between 20 and 100 staff. We have tailored this framework for both these groups by listing the **essential** components for all the above mentioned organisations and then including **recommended** components where a greater level of stringency (for medium-sized organisations) is required.

Privacy is not included in the scope. Matters of privacy are not so much about the protection of an individual's information, but about what information will be shared with others and how much the individual feels in control of this. What information is shared is a decision determined by several factors, namely the patient's wishes, advice from their practitioner, good clinical practice and obligations under New Zealand legislation, which in some instances, e.g. notifiable diseases, requires information to be shared or reported to others. This framework assumes that some personal health information will be shared – it does not say what information should be shared or under what circumstances.

The view of the Committee is that all personal health information is confidential and should be given an equal level of protection⁶. Personal health information is therefore uniformly classified as ‘Medical-in-Confidence’. In deciding classification categories, it was found to be not useful to classify personal health information into different levels of sensitivity because such classifications are context-dependent, largely subjective and can change over time. Refer to Appendix B for further details.

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

- 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 networks⁷.
- Information Privacy, Authentication and Security Framework (PAS) – a set of requirements and recommendations for securing health information, commissioned by the Ministry of Health and ACC. This framework was not implemented and has only been used as a reference by the Committee.
- Aiming for Excellence⁸ – covers off some of the key elements of security of information in General Practice.

Given the existence of these in-sector specific codes of practice and the desire for a fully comprehensive health and disability sector standard, the Committee has decided to use an international security methodology titled ISO/IEC 27002:2006⁹ Information technology – Security techniques – Code of Practice for Information Security Management (ISO 27002). ISO 27002 establishes guidelines and general principles for initiating, implementing, maintaining and improving

⁴ *The Medical Record*, New Zealand Medical Association

⁵ Including other government agencies, schools, insurance companies, etc

⁶ Note that in special circumstances, e.g. a pandemic, Security in Government Sector (SIGS) may require a high level of classification for non-identifiable aggregated health information. Other types of valid classification include Staff-in-Confidence and Commercial-in-Confidence.

⁷ SNZ HB 8169:2002 Health Network Code of Practice, which will be superseded by this series of standards

⁸ *Aiming for Excellence. An Assessment Tool for General Practice. 3rd Edition 2008.* Royal New Zealand College of General Practitioners, New Zealand

⁹ ISO/IEC 27002:2006 was previously numbered ISO/IEC 17799:2006 and is commonly known as “ISO 17799”

security management within any organisation. This is supplemented by a recently published version of the methodology, aimed specifically at health organisations, ISO 27799:2008 Health Informatics – Security management in health using ISO 27002.

A copyright licence to use part of ISO/IEC 27002:2006 in the development of this framework has been obtained. This licence is only applicable to the areas used in this document and are referenced throughout the document as required. Organisations will need to purchase their own copy of the ISO/IEC 27002:2006 if required.

The methodology covers every aspect of security, all of which to some degree apply to health care organisations. Key elements of security covered off in the methodology include:

- an information security policy document;
- allocation of responsibilities for information security;
- awareness, training and education;
- appropriate management of technical environment;
- business continuity management;
- recording incidents and implementing improvements.

This framework selects a set of controls essential for maintaining the minimum level of compliance expected of any organisation holding personal health information in New Zealand.

2.4 Security Controls

There are four ways of managing or “treating” risk. They are to -

1. Accept the risk.
2. Eliminate the risk.
3. Transfer the risk to third parties (insurance, outsourcing or certification).
4. Control the risk to the appropriate level.

The main focus of this standard is on controlling the risk, but it also includes the transfer of risk to third parties through the use of contracts or certification of products. Where the operation of a system is outsourced to a third party provider, then that provider must also comply with this Health Information Security Framework (refer to section 6.5).

Organisations should note that even when some operational risk is transferred to a third party, such as the storage management of personal health information with an outsourced supplier, the responsibility for unauthorised disclosure still remains with the organisation.

The methodology groups security controls into 11 sections. The section headings and a brief description of each are given below.

Section Heading	Description
Information Security Policy Refer section 5	This section explains that an organisation's management requires a policy for security management and that this policy should be reviewed on a regular basis.
Organising Information Security Refer section 6	This section describes what structures, agreements and responsibilities need to be in place to effectively implement information security practices within an organisation.
Asset Management Refer section 7	This section considers information as an asset requiring that health information be classified, handled, labelled and protected appropriately.
Human Resources Security Refer section 8	This section addresses the obligations of employees, contractors and third party users to protect and use information appropriately.
Physical and Environmental Security Refer section 9	This section addresses the physical access controls and appropriate housing for an organisation's information and information processing facilities.
Communications and Operations Management Refer section 10	This section addresses how information processing facilities should be operated in order to maintain adequate security.
Access Control Refer section 11	This section describes how access to information and information processing facilities should be controlled.
Information Systems Acquisition, Development and Maintenance Refer section 12	This section describes how security should be designed into systems, applications and operating procedures.
Information Security Incident Management Refer section 13	This section addresses how security incidents are to be reported, reviewed and learnt from.
Business Continuity Management Refer section 14	This section advises how to mitigate the effects of major systems failures and to make provision for recovery from such failures.
Compliance Refer section 15	This section discusses the obligations required to comply with the standard and legal requirements.

Table 1: Security Control Section Headings

3 Governance and Management Requirements

The diagram below depicts the overall governance and management requirements for the Health Information Security Framework in the New Zealand health and disability sector. Core components are described below.

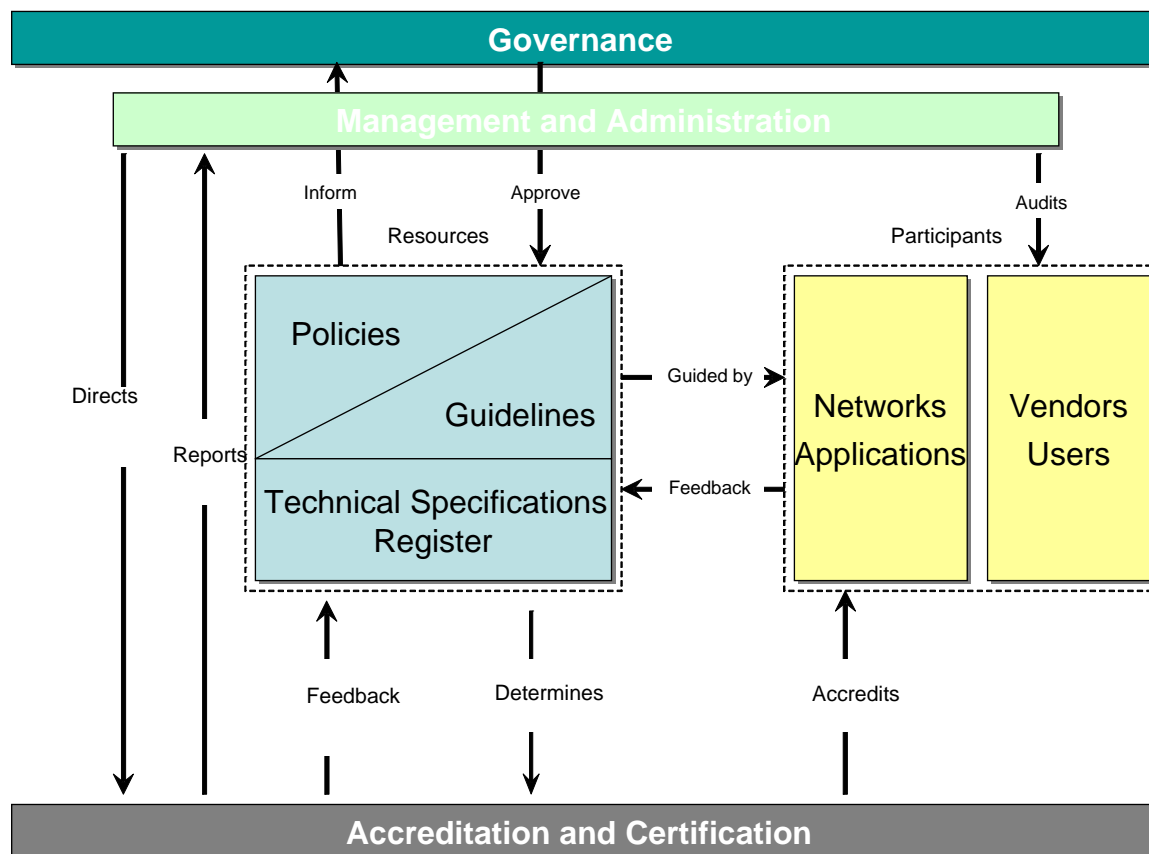


Figure 1: Health Information Security Framework

The Health Information Security Framework is not just a standards publication. It requires governance and management structures to ensure effective implementation. It requires governance to lead, oversee and monitor any resulting changes.

It requires management and administrative support to perform framework and governance body functions such as:

- overseeing a 12-month transition by sector organisations and vendors to achieve compliance (up to three years transition may be needed to achieve “full” compliance);
- developing and implementing security audits;
- resolving disputes and matters of interpretation;
- ensuring risks are identified and treated;
- maintaining and updating the Technical Specifications Register;
- determining consequences for non-compliance;
- providing security advice, training and implementation support for small organisations.

Figure 1 illustrates that networks and applications are accredited and vendors and organisations are audited.

- The Technical Specifications Register identifies the requirements for implementing technical components of the framework. Existing international standards will be used wherever

possible. The Technical Specifications Register is part of a body of knowledge or 'knowledgebase' that supports implementation and includes architectures, other referenced standards, best practice examples, and collaborative tools as endorsed by the governing body from time to time.

- Accreditation and Certification are processes which certify products and services against the framework standards.
- Networks – the communications networks that support access to and exchange of information.
- Applications – the information systems that support collection, access, and exchange of electronic health information.
- Vendors – the suppliers of applications, networks and other services that support collection, access and exchange of information and identity management-related needs, e.g. a telecommunications carrier, or a health care software provider.
- Users – the individuals and organisations entitled to use an application or network to collect, access or exchange electronic health information.

3.1 Governance

A governing body made up of health and disability sector representatives, including consumer representation, is an essential part of implementing the framework for the sector. Governance will provide three key elements for making this framework a success:

1. Leadership to ensure the framework is widely promoted and adopted in the sector. It will set expectations across the sector by raising awareness of security issues and it will help overcome barriers to adopting the framework.
2. Support for a 'living' standard, where elements of interpretation and clarification will lead to incremental and on-going improvements. It will ensure the sector has access to suitable resources and tools so that over the long term, security is embedded into the culture of health organisations.
3. Oversight and monitoring of compliance against the framework. It will monitor the results of self-audits and independent audits to measure how well the sector is doing in meeting the standards. This in turn will reassure the public that security is taken seriously.

Governance is supported by a Management and Administration function that:

- 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

The Committee noted that 'Connected Health', a workstream within the Ministry of Health, has similar governance requirements, including:

- a. Gradual transition period (over one to three years) with audits beginning after 12 months.
- b. Strong health and disability sector representation.
- c. Development and maintenance of a Technical Specifications Register.
- d. Need for product certification and set up of a certification body.

3.2 Accreditation and Certification

The size and complexity of the framework will become too overwhelming if the security requirements for individual products and services provided to the sector have to be checked and monitored by the health organisations themselves. This is beyond the capability and resources of most small health care organisations.

The Committee has therefore opted to provide a means of certifying systems (applications) and networks (services) as meeting the requirements of the security framework by defining a set of criteria against which an accreditation agency can test and measure compliance. Vendors will need to test their health care products against the criteria and publish the results. This will apply to each major release of software product or hardware technology.

The governing body will not actually carry out the compliance audits or certification itself. Health and disability sector organisations will self-certify compliance with the requirements of the Health Information Security Framework and this will be confirmed as part of other accreditation and certification processes. It is envisaged that external agencies will be contracted to perform certification and audits, or that such audits and certification processes will become part of the function of an existing health accreditation or certification body.

4 Structure of the Policies

4.1 Section layout

The following 11 sections of this document are laid out in the same way for readability and consistency, as follows:

Section Heading

This is taken from the ISO 27002 'Section Heading'.

Objective

A short statement summarising the objective or purpose of the section

Policy Statements

A series of policy statements based on ISO 27002 guidelines.

Procedures

A series of action statements representing the precise actions required in order to comply with the policy statements. Each action statement is associated with a participant's role to allow readers of this Framework to quickly identify what they need to do, based on their role.

- Management.
- Administrator.
- User.
- System.

Guidelines

Further advice and guidance, including references to other sources or appendices.

Checklist for Compliance

A checklist of questions which organisations can use to check their level of compliance with the framework. These questions will form the basis for compliance audits.

5 Information Security Policy

5.1 Objective

To provide management direction and support for information security through a security policy.

5.2 Policy Statements

1. An information security policy document is approved by management and published and communicated to all employees and relevant external parties.
2. Management actively supports security within the organisation through:
 - setting a clear policy direction; and
 - demonstrating their commitment; and
 - encouraging a multi-disciplinary approach to security policy.
3. The information security policy is reviewed at planned intervals or when significant new threats arise, to ensure its continuing suitability, adequacy and effectiveness.

5.3 Procedures

Responsibility	Procedure Description	Headline
Management	(a) Create and maintain the Information Security Policy document. It will be reviewed a minimum of every three years. <i>Recommended:</i> Visible support and commitment to security from all levels of management. <i>Recommended:</i> Make available to patients a summary of the security policy.	Create and maintain an Information Security Policy
Administrator	(a) Ensure that all new employees are aware of the Information Security Policy and kept informed of any changes and updates. <i>Recommended:</i> Provide advice and proactively promote the security policy.	Develop employee awareness
User	(a) Read, review, understand and follow obligations under the Information Security Policy.	Follow user obligations
System	(no requirements in this section)	

Table 2: Procedures for Information Security Policy

5.4 Guidelines for Small Organisations

Refer to HISO 10029.2, Section 1 - Sample information security policy for small organisations. Refer to the remaining sections six to 15 in this document for specific guidance.

5.5 Checklist for Compliance

- Does the organisation have an Information Security Policy that was created or last reviewed within the last three years?
- How are employees made aware of the Information Security Policy?

Responsibility	Procedure Description	Headline
System	<p>(a) Allow access to the governance body's health information security website or enable receipt of regular e-mail alerts and updates.</p> <p>(b) Where patients have access to their own information on-line, system controls prevent access to other confidential information held on the system.</p>	Enable health information security alerts

Table 3: Procedures for Organising Information Security

6.4 Guidelines for Small Organisations

Refer to HISO 10029.2, Section 1 – Sample information security policy for small organisations.

Refer to HISO 10029.2, Section 9 – Sample security event/vulnerability reporting form

Refer to HISO 10029.2, Section 9.1 - Sample job description of security administrator.

When assigning responsibility for health information security, the following guidelines should be followed:

- for sole practitioners or very small practices, a senior member of staff should be assigned;
- for small or medium-sized organisations, an information security officer should be nominated, although this does not necessarily need to be a full-time role. Note the information security officer role should be a senior manager rather than an IT systems administrator.

6.5 Agreements for Third Party Access

Often a number of third parties will require access to data or information processing facilities. These can include, but are not limited to, the following:

- locum staff, or temporary professionals or contractors;
- software and maintenance support staff;
- software and hardware vendors;
- student or intern placements;
- volunteers;
- cleaners, caterers;
- other support staff.

Agreements with any third party who can access, process, communicate or manage an organisation's information or information processing facilities should include all relevant health information security requirements and avoid any ambiguity.

Organisations should:

- check their health information security is not compromised by third party requirements in imposed agreements, especially for the release of personal health information.
- review their health information security requirements with suppliers to ensure their security practices are adequate to meet the requirements of this Framework.

Notes on outsourcing

- data could be held in different parts of the country;
- data could be held overseas under different jurisdictions from New Zealand;
- data could be held in locations unknown to the end-user, for example, use of Software as a Service (SaaS) or Cloud Computing;
- patients have a right to know where their data is held;
- if patients request their data to be passed on to a non-audited third party, such as an insurance company or a family member, then the patient is responsible for how their data is protected;

- refer to State Services Commission Guidelines for use of offshore Information and Communications Technology (ICT) providers - <http://www.e.govt.nz/policy/trust-security/offshore-ICT>.

6.6 Checklist for Compliance

- Do the organisation's staff contracts/agreements contain confidentiality clauses?
- Do external parties have confidentiality clauses in their contracts/agreements or have they signed a non-disclosure agreement?
- Do written procedures exist for managing health information security?
- Are employees aware of the written health information security procedures?
- When was the last independent health information security review?
- Who is the organisation's health information security officer?
- What planned and documented actions are there for the remedy of non-compliance?

7 Asset Management

7.1 Objective

The objective is to achieve and maintain an appropriate level of protection for health information and assets.

Regardless of size, it is important that all organisations and sole traders have an inventory or record of assets. Based on this inventory, your business can then provide levels of protection commensurate with the value and importance of the health information and assets used to maintain and house health information.

7.2 Policy Statements

1. All personal health information is classified as 'Medical-in-Confidence' and therefore treated as confidential.
2. Systems associated with information security such as software, hardware, supporting utilities, etc. and the information itself, are considered to be assets.
3. All assets are accounted for and have a nominated person or custodian who is responsible for the proper protection and acceptable use of the asset.
4. Information assets comprise all storage and communication media, including printed material (see Appendix C for types and risk assessment).

7.3 Procedures

Responsibility	Procedure Description	Headline
Management	<p>(a) Create and maintain an inventory of assets associated with the protection of health information in an asset register.</p> <p>(b) Document and implement rules for acceptable use of health information and associated assets. Refer section 8 and section 9.</p> <p><i>Recommended:</i> Assign ownership to designated parts of the organisation and delegate routine tasks to custodians.</p>	Maintain Asset Register
Administrator	<p>(a) Label, file and handle all personal health information stored on media as 'Medical-in-Confidence'. Additional controls may be necessary for some patients or subsets of information.</p> <p>(b) Ensure physical assets are sanitised (have information fully removed) prior to disposal. Paper or other physical media should be physically destroyed.</p> <p><i>Recommended:</i> Inventory checks should be carried out annually.</p>	Handling 'Medical-in-Confidence' information Safe disposal of assets
User	<p>(a) Conform to acceptable use of health information guidelines. Refer HISO 10029.2, Section 6 – Sample Security Access Agreement</p> <p>(b) Justify access to personal health information.</p>	

Responsibility	Procedure Description	Headline
System	<p>(a) Label and file all personal health information as "MEDICAL-IN-CONFIDENCE". This includes all personal health information printed on paper or held on portable storage media</p> <p>(b) There may be additional controls which are necessary for some patients or subsets of information</p> <p><i>Recommended: Access Control should be applied to electronic files.</i></p>	"Medical-in-Confidence" Labelling

Table 4: Procedures for Asset Management

7.4 Guidelines for Small Organisations

Disposal of physical assets may be contracted out to an external party.

Where additional health information security controls are necessary, an option is **not** to hold personal health information in a shared computer system.

Physical output from the system, including printed reports and electronic removable media should be labelled or stored in files marked as 'Medical-in-Confidence'.

Refer to HISO 10029.2, Section 5 – Sample template for asset register.

Information assets include software, hardware, supporting utilities, databases, data files, contracts and agreements, system documentation, research information, user manuals, training material, operational and support procedures, business continuity plans, operational staff knowledge, audit trails, paper records, patient information and archived information.

7.5 Guidelines for Retention/Disposal of Health Information

Organisations that are public offices must comply with the Public Records Act 2005. Public offices are the legislative, executive and judicial branches of government. They include Crown Entities, such as District Health Boards.

Under the Act:

- All public offices are required to create and maintain full and accurate records in accordance with normal, prudent business practice. This includes activities carried out by contractors on a public sector organisation's behalf. These records must also be accessible over time.
- Public offices may only dispose of their records with the Chief Archivist's authorisation. Disposal is the archival term for the ultimate fate of records; usually either by destruction or transfer to archives. A public office can obtain a disposal authority from the Chief Archivist for records specific to its functions. A General Disposal Authority for District Health Board Records that covers clinical and non-clinical records has been approved by the Chief Archivist.

The Public Records Act 2005 does not apply to entities, such as PHOs and NGOs, which are not public offices. However, the Health (Retention of Health Information) Regulations 1996 applies to all providers of health and disability services. The Regulations require all providers of health and disability services to retain information relating to an identifiable individual for a minimum period of 10 years after the most recent date, as shown in the health information, on which health or disability services were provided to that individual. The obligation rests on the provider that for the time being holds the health information, even though the information may have been transferred to that provider. The obligation to retain health information ceases if the provider transfers the information to another provider or to the individual concerned.

7.6 Checklist for Compliance

- Does an asset register exist?
- Is there evidence that the asset register has been checked and updated?
- Do guidelines exist for the acceptable use of health information?
- Has personal health information been labelled 'Medical-in-Confidence'?

8 Human Resources Security

8.1 Objective

To ensure that employees, contractors and third party users:

- abide by organisational health information security policy and procedures in the course of their normal work; and
- understand their responsibilities and the health information security requirements of their roles; and
- help prevent loss or misuse of health information through theft, fraud or misuse of facilities; and
- have health information security rights reviewed or terminated after a change of employment or role.

Staff play the most crucial role in the protection of personal health information. Patients expect their health information to be kept confidential and secure by any staff handling it.

8.2 Policy Statements

1. All Human Resource policies and procedures and employees' terms and conditions incorporate information security requirements, including the following:
 - to act in accordance with the organisation's health information security policy;
 - to protect assets from unauthorised access, disclosure, modification, destruction or interference;
 - to report actual or potential health information security events or risks.
2. All candidates for employment are appropriately screened, especially for sensitive jobs.
3. Management ensures that employees, contractors and third party users apply health information security in accordance with the established policy and procedures.

8.3 Procedures

Responsibility	Procedure Description	Headline
Management	<ul style="list-style-type: none"> (a) Ensure new employees and temporary staff are screened appropriately. (b) Include health information security responsibilities in job descriptions, terms and conditions of employment, and employee induction. (c) Authorise changes of role and associated access rights. (d) Have a formal disciplinary process for employees who have breached health information security. (e) Ensure that all parties receive appropriate health information security awareness education and training relevant to their job function. 	<p>Screen new staff</p> <p>Include health information security in job descriptions</p> <p>Awareness training</p>
Administrator	<ul style="list-style-type: none"> (a) Follow procedures for creating and removing users' access. (b) Ensure a user's access rights are reviewed and amended accordingly on change of role and/or responsibilities within the organisation. (c) Ensure users have received appropriate health information security awareness training before they are provided with their system access. (d) Ensure return of all equipment and removal of all access rights on termination of employment. 	Maintain users access rights
User	<ul style="list-style-type: none"> (a) Act in accordance with the health information security policies and procedures. (b) Sign security policy/responsibility agreement to show that they have read, understood and accepted the security policy. (c) Return all assets (hardware, information, processing facilities, printed or other copies) upon exiting the organisation/role. (d) Sign employment agreement, which includes health information security responsibilities. (e) Attend induction course which covers appropriate health information security awareness, education and training relevant to their job function. (f) Be aware of how to report a health information security incident. 	<p>Sign security agreements</p> <p>Return equipment</p> <p>Attend Induction course</p>
System	<i>Recommended:</i> Uses role-based security to maintain access rights.	

Table 5: Procedures for Human Resources Security

8.4 Guidelines for Small Organisations

Refer to 10029.2, Section 6 - Sample security access agreement.

Refer to 10029.2, Section 8 - Sample employee/contractor exit checklist.

The employee's responsibilities regarding confidentiality, data protection, ethical use of data and appropriate use of the organisation's equipment and facilities should be documented in the employee's job description, employment agreement and/or security agreement.

The screening process should include:

- character and employer reference checks;
- validation of their formal qualifications;
- independent identity verification, e.g. sighting of passport, drivers licence;
- check on criminal record (police check) for sensitive positions; for full privacy requirements refer to <http://www.privacy.org.nz/privacy-at-work-a-guide-to-the-privacy-act-for-employers-and-employees/>

8.5 Checklist for Compliance

- Is there a checklist for removal of access rights when employees leave or change role?
- Are the health information security requirements documented as a part of job descriptions and terms and conditions of employment?
- Is there evidence that all staff have received education and induction courses?
- Does the employee induction programme include health information security requirements?
- Have staff signed their health individual security policy agreements?
- Do staff know how to report a health information security incident?

9 Physical and Environmental Security

9.1 Objective

To prevent unauthorised physical access, damage or interference to the organisation's premises and information assets.

Precautions need to be undertaken to ensure the organisation is adequately protected against physical and environmental damage to information and reduce the risks of theft of equipment, physical impairment, unauthorised disclosure of information, compromised system integrity and disruptions to service.

9.2 Policy Statements

1. Information processing and storage facilities are housed in secure areas with appropriate entry controls and are protected from unauthorised access, damage and interference.
2. Equipment is sited or protected to reduce the risks from environmental threats or hazards, e.g. power failures, overheating, water damage, fire or dust.
3. Equipment is correctly maintained to ensure its continued availability and fitness for purpose.

9.3 Procedures

Responsibility	Procedure Description	Headline
Management	<p>(a) Secure areas that contain personal health information and information processing facilities by restricting or supervising physical access.</p> <p>(b) Provide secure offices, rooms and facilities and reasonable protection against damage from fire, flood, earthquake or other forms of environmental hazard.</p> <p>(c) Authorise off-site use of equipment, software or information.</p> <p><i>Recommended:</i> Make provision for private areas where sensitive information can be discussed.</p> <p><i>Recommended:</i> Medium to large organisations should have their own controlled room to hold critical computer equipment (servers, network).</p>	<p>Restrict physical access</p> <p>Protect equipment from hazards</p>
Administrator	<p>(a) Check computer equipment containing storage media to ensure that any health information and software are rendered non-retrievable¹⁰ prior to disposal or re-use.</p> <p>(b) Maintain equipment appropriately (including regular health checks) to ensure its continued availability and fitness for purpose.</p>	<p>Maintain equipment</p>
User	<p>(a) Do not leave printed personal health information in a place where unauthorised users may view it.</p> <p><i>Recommended:</i> Work in a secure area when necessary for the task in hand.</p> <p><i>Recommended:</i> When working off-site, at home or in other public areas, use of portable computers and storage media</p>	<p>Working off-site</p>

¹⁰ Storage devices can either be physically destroyed, or wiped by special software which wipes out all traces of the original data by overwriting it several times

¹¹ The Portable Use Policy (part of the Technical Specifications Register) is under development.

Responsibility	Procedure Description	Headline
	should be operated in accordance with a Portable Use Policy. ¹¹	
System	<p>(a) Install a burglar alarm and a fire alarm on the premises.</p> <p><i>Recommended:</i> Control and monitor access to restricted areas electronically, e.g. via card system, or camera.</p>	

Table 6: Procedures for Physical and Environment Security

9.4 Guidelines for Small Organisations

Consider the following when securing your premises:

- ensure adequate locks on all access doors and record who has the keys;
- place bars or security locks on windows;
- install a working burglar and fire alarm system;
- have receptionist staff at the point of entry.

9.5 Checklist for Compliance

- Is data fully wiped from equipment containing storage media when disposed of or re-used?
- Is there restriction of physical access to areas where personal health information is held?
- Are physical equipment and storage media stored securely and protected from environmental damage?
- Are there procedures in place to ensure alarms are checked regularly?
- Is the Portable Use Policy for the use of laptops and remote devices, including phones, understood?

10 Communications and Operations Management Policy

10.1 Objective

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

Data integrity is concerned with the preservation of information and data whilst being stored, used, transferred and retrieved. The organisation must be confident that the information has not been tampered with or modified, other than as authorised. Data integrity in the organisation's computer systems and databases is especially important, because corruption of data could result in risk to life or loss of reputation. Insufficient control of changes to information systems is a common cause of system and security failure.

10.2 Policy Statements

1. The organisation has an easily accessible and available Operating Procedures manual which documents:
 - backup procedures; and
 - computer start-up and close down procedures; and
 - system restart and recovery procedures; and
 - equipment maintenance functions; and
 - changes made to systems; and
 - instructions for handling errors; and
 - management of audit trail and system log information.
2. Use of external support and implementation services is covered by appropriate contracts, including Service Level Agreements.
3. Protection against malicious software such as viruses and malware is implemented. Procedures are in place to ensure protection software is properly updated and maintained.
4. Backups are used to maintain the integrity and availability of information and of information processing facilities.
5. Appropriate operating procedures are established to protect documents, removable storage media, printed information and system documentation from unauthorised disclosure, modification, removal and destruction.
6. When personal health information is exchanged over a network, it is protected from interception, incorrect routing and loss. When personal health information is exchanged on physical media, it is protected from unauthorised access, misuse or corruption.
7. Systems are monitored, and operator and fault logs checked to ensure that information system problems are identified.

10.3 Procedures

Responsibility	Procedure Description	Headline
Management	<ul style="list-style-type: none"> (a) Formally authorise all major changes to systems. (b) Use a Secure Health Network¹² for the exchange of personal health information or online access. (c) Ensure that data is adequately backed up and stored in a protected location. <p><i>Recommended:</i> Keep separate application environments for development, test and production systems.</p> <p><i>Recommended:</i> Check the 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.</p> <p><i>Recommended:</i> Segregate duties to reduce opportunities for misuse of information assets.</p>	<p>Back up data</p> <p>Monitor third party agreements</p>
Administrator	<ul style="list-style-type: none"> (a) Document operating procedures in a manual, including how to dispose of media safely and how to encrypt data on portable media. (b) Ensure there is sufficient capacity with information systems to support good system performance and reliability. (c) Take backup copies of information and software, test restoration of data regularly and store in an encrypted format at a secure off-site location. (d) Implement anti-malware (includes anti-virus) software on all servers and workstations and ensure it is kept up-to-date. (e) Implement and operate a Secure Health Network according to your network services agreement, to ensure the protection of information in networks and supporting infrastructure. (f) Test new versions of software and facilities before deployment. <p><i>Recommended:</i> Vendors should produce evidence of adequate laboratory testing or show evidence of certification, before deploying new versions and facilities, or provide on-site test facilities to enable pre-deployment testing to take place.</p> <p><i>Recommended:</i> Develop suitable acceptance test scripts for systems during changes and upgrades to systems.</p> <p><i>Recommended:</i> Where data is archived or kept for historical purposes, ensure it is stored in an open format, and is readable and retrievable after 10+ years.</p> <p><i>Recommended:</i> Where systems intercommunicate, carry out end-to-end testing of the communication, including validation to ensure it was received correctly.</p>	<p>Manage information systems capacity</p> <p>Back up and restoration</p> <p>Implement up-to-date anti-virus software</p> <p>Test new versions</p>

¹² A Secure Health Network is a network connection between organisations or persons built and operated according to the technical specifications required to securely access or exchange personal health information

Responsibility	Procedure Description	Headline
User	(a) Be aware of the dangers of viruses and malware and report problems arising. (b) Do not make changes to systems or software without administrator or management approval. (c) Do not send patient identifiable information or attachments over unsecured email (remove identifying information). (d) Ensure media which are physically stored or transported off-site are in an encrypted format.	Report problems Use email appropriately Take appropriate portable media precautions
System	(a) Ability to write data to portable storage media in encrypted format. (b) Ability to use standards-based messaging. (c) Ability to log and/or alert data integrity faults generated by the system. (d) Ability to synchronise system clock to an agreed accurate time source. <i>Recommended:</i> Ability to “wipe” hard disk data by overwriting a number of times before re-use or disposal. <i>Recommended:</i> Disable the ability to change time on local device. <i>Recommended:</i> Provide security for the transmission of email, text/video messaging, or instant messaging systems which handle personal health information.	Portable media encryption Use of alerts Secure email and messaging

Table 7: Procedures for Communications and Operating Management Security

10.4 Guidelines for Small Organisations

The organisation’s senior staff need to have knowledge of the administrator access userID/password.

Organisations should be aware that software that has already been released elsewhere may not be stable in their environment and that testing is therefore vital.

Testing will be dependent on the risks assessed.

Refer to HISO 10029.2, Section 3 – Backup policy guidelines.

Refer to HISO 10029.2, Section 4 – Sample backup procedure.

Encryption Standards – Refer to HISO 10029.3, Technical Specifications Register

Use of email:

- normal email is stored in an unencrypted format on the Internet Service Provider’s server and is therefore readable by third parties;
- email containing personal health information should be encrypted or secured in some manner;
- email, paper copy or fax from provider to patient or other source is allowable so long as the patient has consented to sending the information via non-secure route.

10.5 Checklist for Compliance

- Is there an Operating Procedures manual covering off health information security policy requirements?
- Are the right people aware of, and using, the Operating Procedures manual?

- Is there a separate test environment for each application?
- Are faults logged and checked?
- Is secure messaging used for the transfer of personal health information?
- Are daily backups taken?
- Are backups stored off-site in an encrypted format?
- Has the restoration from a backup been tested in the last three months?
- Is health information / data on portable media encrypted?

Responsibility	Procedure Description	Headline
	<p>termination of employment or change of role.</p> <ul style="list-style-type: none"> (b) Assign each user a unique ID which is not re-used and a password which is kept confidential to the user (assign a temporary password which the user is forced to change immediately). (c) Ensure any wireless access points on the internal network are secured to the standard required by HISO 10029.3 Technical Specification Register. (d) Password-protect and encrypt information on devices used off-site, including laptops, mobile devices, home computers or portable media. (e) Use a Secure Health Network and ensure that customer side network access points are secure. (f) Use multi-factor authentication¹³ to control access for remote users. (g) Enforce passwords to change at regular intervals. (h) Enforce passwords to be of minimum length as per the access control policy and HISO 10029.3 Technical Specification Register. (i) Enforce lockout of login access after a fixed number of login attempts, as per the HISO 10029.3 Technical Specification Register. (j) Create passwords to privileged accounts (Administrator access) that meet or exceed HISO 10029.3 Technical Specification Register. <p><i>Recommended:</i> Develop a procedure to provide and revoke access rights at short notice, to support the requirements for locums and others for temporary access.</p> <p><i>Recommended:</i> Regularly review audit trails of access and activity – perform in depth audits and pay special attention to external parties.</p> <p><i>Recommended:</i> Maintain a register of telework and mobile devices.</p>	<p>Assign unique passwords</p> <p>Secure wireless networks</p> <p>Secure external network</p> <p>Audit access and usage</p>
User	<ul style="list-style-type: none"> (a) Follow good practice in the selection and use of passwords (see guidelines). (b) Change passwords as required by the information security policy. (c) Read, review and understand obligations under the Access Control Policy (such obligations may be included in the user's signed security agreement). (d) Accept responsibility for all access under their credentials and ensure access is appropriate for their duties. (e) Do not share or disclose passwords. (f) Report any security breach. (g) Prevent any inadvertent or unauthorised release of information, particularly from unattended equipment, by terminating active sessions, locking the screen or logging off when finished. (h) Log off or terminate active sessions when finished and close down computer at end of the day. (i) Comply with mobile computing and teleworking policy. 	<p>Use good passwords</p> <p>Report breaches</p> <p>Log off computer</p>

Responsibility	Procedure Description	Headline
System	<p>(a) Allow users to select and change their own passwords and include a confirmation procedure to allow for input errors.</p> <p>(b) Prevent reuse of previous user passwords.</p> <p>(c) Keep audit trail of all login attempts to the system.</p> <p>(d) Store and transmit passwords in an encrypted format.</p> <p>(e) Automatically close down or terminate a session after a fixed time period of user inactivity.</p> <p>(f) Support access to a Secure Health Network.</p> <p>(g) Support a minimum standard specified in HISO 10029.3 Technical Specification Register on wireless networks.</p> <p>(h) Access the internet via a firewall.</p> <p><i>Recommended:</i> Provide a role-based access control system.</p> <p><i>Recommended:</i> Keep audit trail of all user activity within an application – this includes view-only activity.</p> <p><i>Recommended:</i> Allow viewing and analysis of audit trail activity by approved users. Restrict and record the ability to delete or modify log files.</p> <p><i>Recommended:</i> Applications should enable control of user access rights at each level of access, e.g. read, write, delete and execute.</p> <p><i>Recommended:</i> Applications should use menus or tabs to control (or hide) access to application system functions.</p> <p><i>Recommended:</i> Enforce change of passwords at regular intervals as required by the information security policy.</p>	Password protection

Table 8: Procedures for Access Control

11.4 Guidelines for Small Organisations

Be aware of the risks of giving third party suppliers or vendors administrative level access rights to applications and servers.

For the use of locums, the access rights can be retained in the system if the locums are going to be employed intermittently over an extended period of time.

Refer to HISO 10029.2, Section 1 - Sample information security policy for small organisations (in particular the section on remote access).

Password use: good secure practices should be followed in the selection and use of passwords including:

- keeping passwords confidential;
- changing passwords at regular intervals (minimum annually);
- not keeping written records of passwords, unless these are stored securely;
- not choosing passwords which can be easily discovered, e.g. date of birth, or name of family member;
- using a combination of numeric, alphabetical and case sensitive characters.

Clear Desk and Clear Screen Policies: good security practices should be followed in the display of personal health information, either on paper or on computer workstations including:

- removing from sight all personal health information, whether on paper or on electronic storage media, when not required or while the office is unattended.
- logging off or screen locking computers and terminals when unattended or not in use.

11.5 Checklist for Compliance

- Does the organisation have an access control policy for its applications?
- Is there evidence of security audits of user's access, including reviewing attempts at login?
- Do guidelines for creation of passwords exist?
- Are user access rights regularly reviewed?
- Are new users approved and old users removed?
- Does the organisation have a policy covering mobile computing and teleworking?¹⁴
- Are passwords allocated securely and kept secure?
- Does the organisation have a Clear desk and Clear Screen policy?

¹⁴ Policy under development

12 Information Systems Acquisition, Development and Maintenance

12.1 Objective

To ensure that health information security is an integral part of information systems design and operation.

12.2 Policy Statements

1. Statements of business requirements for new information systems, or enhancements to existing information systems specify the requirements for security controls.
2. Input and output processing controls are incorporated into applications to ensure data integrity, including:
 - validating data input; and
 - detection of internal corruption of data through processing errors or deliberate acts; and
 - ensuring authenticity and protection of message integrity; and
 - validating data output.
3. Timely information about technical vulnerabilities of information systems being used is obtained and appropriate measures taken to address the associated risk.

12.3 Procedures

Responsibility	Procedure Description	Headline
Management	<p>(a) Selection criteria for new systems will favour those systems which are certified (refer to HISO 10029.3, Technical Specifications Register).</p> <p><i>Recommended:</i> Security requirements should be identified and agreed prior to the development, acquisition and/or implementation of information systems.</p>	Certification of systems
Administrator	<p>(a) Apply software patches (both application and operating system) to remove or reduce security weaknesses as part of a regular maintenance cycle.</p> <p><i>Recommended:</i> Regularly check appropriate sources of information about technical vulnerabilities.</p> <p><i>Recommended:</i> Where cryptographic controls¹⁵ are used, keys should be protected against modification, loss, destruction and unauthorised disclosure.</p>	Apply security patches
User	(no requirements in this section)	
Systems	<p>(a) Systems must have controls to ensure data input validation, checks on loss of data integrity as a result of processing failures, message integrity and data output validation.</p> <p>(b) Systems support data integrity audits where messages are traceable and reportable.</p> <p><i>Recommended:</i> Operating system services should be locked down to minimise the risk of vulnerabilities.</p>	Preserve of data integrity

Table 9: Procedures for Information Systems Acquisition, Development and Maintenance

¹⁵ Cryptographic control is the ability to render plain text unreadable and re-readable (encrypt and decrypt) using cryptographic techniques. Cryptographic controls are also used to ensure integrity and non-repudiation

12.4 Guidelines for Small Organisations

Cryptographic controls can be used to achieve security for confidentiality, integrity/authenticity and non-repudiation.

System maintenance may be contracted out to an external party.

12.5 Checklist for Compliance

- Is there evidence of receipt of and appropriate response to vendor warnings of technical vulnerabilities?
- Are the products or systems being used certified for their security functions?
- Are cryptographic keys kept in a secure manner?

13 Incident Management

13.1 Objective

To manage health information security events and weaknesses in a consistent and effective manner.

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.

13.2 Policy Statements

1. Health information security events and weaknesses associated with information systems are notified allowing timely corrective action to be taken.
2. Management actively support the management of health information security events and weaknesses by:
 - having formal event monitoring, reporting and escalation procedures in place; and
 - making users, contractors and third parties aware of their responsibilities to notify security breaches and weaknesses as quickly as possible; and
 - having a formal discipline process established; and
 - having a single point of contact for reporting security breaches and weaknesses which is known, always available and able to provide adequate and timely response; and
 - having responsibilities and procedures in place to handle information security events and weaknesses effectively once they have been reported.
3. Procedures are established to handle different types of health information security incidents, including:
 - information system failures and loss of service;
 - malicious code (viruses, malware);
 - denial of service attacks;
 - errors resulting from incomplete or inaccurate data;
 - breaches of confidentiality and integrity;
 - misuse of information systems.

13.3 Procedures

Responsibility	Procedure Description	Headline
Management	<p>(a) Respond to reported security events and weaknesses in a quick, effective and orderly manner.</p> <p>(b) Notify vendors and/or certifying bodies of failures in system security controls.</p> <p>(c) Notify all affected parties of the security incident and possible consequences e.g. loss of data integrity.</p> <p><i>Recommended:</i> Develop formal event monitoring, reporting and escalation procedures to enable the types, volumes and cost of incidents to be monitored.</p> <p><i>Recommended:</i> Institute a process for continual learning and developing improvements from monitoring security incidents.</p> <p><i>Recommended:</i> Facilitate protection and collection of evidence related to a security event involving staff disciplinary or legal action.</p> <p><i>Recommended:</i> Develop policy to handle duress situations.</p>	Notify affected parties of security incidents
Administrator	<p>(a) Follow instructions from management for recording and monitoring security incidents.</p> <p>(b) Implement business continuity plans if needed.</p> <p>(c) Report any weaknesses identified and security events as they occur.</p> <p><i>Recommended:</i> Monitor system and alert logs for potential health information security breaches and weaknesses.</p> <p><i>Recommended:</i> Educate users, contractors and third parties in how to report security incidents.</p>	<p>Record, monitor and report on security incidents</p> <p>Implement business continuity plans</p>
User	<p>(a) Report security events and weaknesses through appropriate channels as quickly as possible and in a confidential manner.</p>	Report security events
System	<p>(a) Log and alert significant events indicating health information security breaches and weaknesses.</p>	Log and alert

Table 10: Procedures for Incident Management

13.4 Guidelines for Small Organisations

Refer to HISO 10029.2, Section 9 - Sample security event/vulnerability reporting form.

Refer to the Privacy Breach Guidelines issued by the Privacy Commissioner (available at <http://www.privacy.org.nz/assets/Files/Privacy-Breach-Guidelines/Privacy-breach-guidance.DOC>).

Examples of health information security incidents are:

- suspicious use of or access to patient information;
- loss or deletion of all of or parts of the patient's medical record;
- intrusion into system resulting in compromise of security or loss of confidentiality;
- malfunctions or other anomalous behaviour of the system (possibly indicating external attack);
- wrong information entered into system or sent to an unauthorised party as a result of human error;
- theft of equipment or files;

- loss of availability of system or damage to computer equipment.

13.5 Checklist for Compliance

- Do formal event monitoring, reporting and escalation procedures exist?
- Are users, contractors and third parties made aware of the procedures and their obligations for reporting security incidents and/or weaknesses?
- Provide evidence of a previous health information security event and show that procedures were followed.
- Do formal procedures to report the loss of patient records or other privacy breaches exist?

14 Business Continuity

14.1 Objective

To minimise the effect of major failures of information systems or physical disasters.

Business Continuity Management is concerned with ensuring that your business and business functions are able to continue in the event of environmental, human or technical failures. It is focused on two controls: prevention and recovery. Where health information required for the treatment of a patient is stored in a computer system, it is crucial for your business to maintain availability.

14.2 Policy Statements

1. Management understands the risks and potential impacts the organisation faces as a result of a major failure of information systems or physical disasters including:
 - identification of acceptable loss of health information and services;
 - identification of acceptable time frame to full recovery;
 - procedures to recover and restore business operations and availability of information;
 - identification of the triggers and threats which will cause the business continuity plan to be activated.
2. Management shall develop and implement a business continuity management process including a business continuity plan, to support the above.

14.3 Procedures

Responsibility	Procedure Description	Headline
Management	(a) Develop Business Continuity Plan (BCP), including Disaster Recovery planning. (b) Ensure the Business Continuity Plan is updated when a system or risk changes and is reviewed at least annually. <i>Recommended:</i> Consult with other providers/organisations in region. <i>Recommended:</i> Perform a risk assessment to identify events which could cause business interruptions, along with their probability and impact. <i>Recommended:</i> Identify an alternative processing site with the appropriate security measures and equipment.	<u>Develop BCP</u> <u>Review BCP</u>
Administrator	(a) Locate hardcopy of BCP in an easy to find on-site location and a copy off-site. (b) Test BCP at regular intervals, at least annually.	<u>Test BCP</u>
User	(a) Educate and involve users in preparing and testing the Business Continuity Plan.	<u>Test BCP</u>
System	(a) Allow restoration of data and systems from backup.	

Table 11: Procedures for Business Continuity

14.4 Guidelines for Small Organisations

Refer to HISO 10029.2, Section 2 - Sample business continuity plan for small organisations.
 Refer to HISO 10029.2, Section 4 - Sample backup procedures.

14.5 Checklist for Compliance

- Does the Business Continuity Plan, including Disaster Recovery, exist?
- Is there a record of test restores?
- Is a copy of the Business Continuity Plan stored off-site along with your backup tapes and software?
- Have manual workarounds been documented in case of temporary loss of systems?
- Has an alternative site been identified with the correct security measures and equipment?

15 Compliance

15.1 Objective

To avoid breaches of any law, statutory, regulatory or contractual obligations and of any health information security requirements.

To ensure compliance with health information security policies and standards.

To use audit processes effectively and minimise disruption to the business.

15.2 Policy Statements

1. The design, operation, use and management of information systems will be subject to statutory, regulatory, or contractual security requirements and should respect intellectual property agreements. The major regulatory requirements to be considered are:
 - Health Act 1956
 - Privacy Act 1993
 - Crime Act 1961
 - Health Practitioners Competence Assurance Act 2003
 - Public Records Act 2005
 - Mental Health (Compulsory Assessment and Treatment) Act 1992
 - Electronic Transactions Act 2002
 - Injury Prevention, Rehabilitation, and Compensation Act 2001
2. Important relevant codes and guidelines include:
 - Code of Health and Disability Services Consumers Rights
 - NZMA Code of Ethics
 - NZNO Code of Ethics
 - Pharmacy Council Code of Ethics
 - Health Information Privacy Code 1994

There may be other acts or codes related to professional groups or business operations.
3. The security of information systems is regularly reviewed and audited against the Health Information Security Framework and the security policy and procedures which have been developed by the organisation.
4. There are controls to safeguard operational systems and audit tools during information systems audits. Protection is also required to safeguard the integrity and prevent misuse of audit tools.

15.3 Procedures

Responsibility	Procedure Description	Headline
Management	(a) Comply with legislation and regulations around the intellectual property rights of software and information. (b) Store and dispose of organisational records in accordance with the requirements of the Public Records Act General Disposal Authority for health information or Retention of Health Information Regulations (see section 7.5). (c) Perform a structured self-audit against the Health Information Security Framework annually. <i>Recommended:</i> Take legal advice on legislative requirements if necessary.	<u>Comply with relevant legislation</u>
Administrator	(a) Advise users that their access will be monitored. <i>Recommended:</i> Provide notice or “splash” screen to users concerning compliance with security protocols each time they log into the system.	<u>Monitor user access</u>
User	(a) Use systems for legitimate business purposes or approved use. (b) Comply with software copyright agreements including downloaded files. (c) Where possible, inform the patient before transfer of personal health information to external organisations.	<u>Comply with relevant legislation and agreements</u>
System	<i>Recommended:</i> Apply system controls to protect against inappropriate use where possible.	

Table 12: Procedures for Compliance

15.4 Guidelines for Small Organisations

Refer to the relevant professional body for advice or guidance on ethical issues.
 Refer to the organisation’s legal advisor for advice or guidance on interpretation of legislative requirements.

15.5 Checklist for Compliance

- Has a security compliance self-audit taken place in the last year?

Appendix A – Glossary

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

Term	Definition
Accountability	A is accountable to B when A is obliged to inform B about A's (past or future) actions and decisions, to justify them and to suffer punishment in the case of eventual misconduct.
Accredited Certification Body	A designation earned by an organisation to assure that it is qualified to perform a job or task.
Accredited off-the-shelf	An information system or technology product which can be procured from an accredited supplier, which has been certified as complying with a specified set of requirements and which remains compliant when installed as supplied.
Asset register	A list that records assets, their description and location.
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 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) A copy of data made for the purpose of recovery. (verb) To make a copy of data for the purpose of recovery.
Business Continuity Plan (BCP)	Business Continuity is creation of a plan for how an organisation will recover and restore partially or completely interrupted critical functions, aimed at allowing the organisation to continue functioning after (and ideally, during) a disaster, rather than simply being able to recover after a disaster.
Classification	Accords different levels of protection based on the expected damage, prejudice and/or loss the health information might cause in the wrong hands.
Clinician	Medical professionals who are engaged in actual patient care as opposed to researchers and academics.
Cloud Computing	Computer storage and processing power that is accessible over the internet and able to be connected by anyone from either work, home or via mobile devices
Confidentiality	Information is not available or disclosed to unauthorised individuals, entities, or processes.
Cryptography	Transforming usable information into a form that renders it unusable by anyone other than an authorised user; this process is called encryption.
Custodian	In the health information security context a custodian is a person entrusted with the custody or care of a person's health information.
Data elements	An atomic piece of data, e.g. "first name", "last name", etc.
Data group	Group of data elements of related data, e.g. "patient identification", "demographic data".

Term	Definition
Disaster Recovery	Disaster Recovery is the process, policies and procedures related to preparing for recovery critical to an organization after a natural or human-induced disaster. Disaster recovery planning is a subset of a larger process known as business continuity planning and should include planning for resumption of applications, data, hardware, communications (such as networking) and other IT infrastructure
Environmental threats or 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.
External party (also 3rd party)	Parties not directly involved in the care of patient, with whom the provider has a business relationship (e.g. an IT vendor).
Fax	Transmission of a facsimile image from one fax machine to another.
Facility	A single physical location from which health goods and/or services are provided. A health care provider organisation may consist of multiple facilities.
Firewall	A firewall is 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.
GP	General Practitioner.
GP2GP	The General Practitioner to General Practitioner Patient Notes Transfer Project.
Health care provider	A person, facility or organisation that provides 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.
HISAC	The Health Information Strategy Advisory Committee.
HIS-NZ	Health Information Strategy for New Zealand.
ICT	Information and Communications Technology
Integrity	(Of data); data must not be altered or destroyed in an unauthorised manner and accuracy and consistency must be preserved regardless of changes.
Interoperable	The ability of products, systems, or business processes to work together to accomplish a common task. Interoperability must deliver mechanisms for organisational inter-working from technical, information and business perspectives but not necessarily prescribe how those mechanisms are used to deliver to emerging requirements. 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.
Medical-in-Confidence	An information security classification given to personal health information.
MoH	Ministry of Health
NZMA	New Zealand Medical Association
NZMC	The Medical Council of New Zealand
NZNC	The Nursing Council New Zealand

Term	Definition
NZNO	New Zealand Nurses Organisation
Patient	Any person who receives medical attention, care, or treatment.
Personal health information	Personal health information is health information identifiable to an individual.
PMS	Patient Management System or Practice Management System.
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, cellphones, iPods etc.).
Practitioner	Some one who engages in a health care related occupation.
Primary care	The activity of a health care provider who acts as a first point of consultation for all patients.
Procedure	A specification of 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 (e.g. emergency procedures).
Risk Management	Risk Management is the identification, assessment, and prioritisation of risks and includes utilising resources to minimise, monitor, and control or impact of these risks.
RNZCGP	Royal New Zealand College of General Practitioners.
Secure email	Email which is encoded or encrypted in transit.
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
Sector	Health and disability sector.
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)	Software as a Service
Micro, small, medium, large organisations	Micro-organisations (fewer than 5 staff), small organisations (6-49) and medium organisations (50-100), and large organisations (>500).
System message	A message for machine consumption that is automatically initiated by a trigger event, e.g. electronic receipt of a referral which is then transmitted to the originator of the event, i.e. without intervention by any user.
Systems	Application or electronic business process which supports collection, access, processing and exchange of personal health information.
Teleworking	A work arrangement in which employees enjoy flexibility in working location, that is a central place of work is supplemented by a remote location (e.g. home), usually with the aid of information technology and communications.
Treatment	The act of remediation of a health problem.
Virus	A computer virus is 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.

Term	Definition
Worm	A computer worm is a self-replicating computer programme. It uses a network to send copies of 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.
WPA2	Wi-Fi Protected Access (WPA2) is a certification programme administered by the Wi-Fi Alliance to indicate compliance with the security protocol created by the Wi-Fi Alliance to secure wireless computer networks.

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 risk assessment of how much damage, loss or prejudice would result from compromising specific content, and 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:

- In Confidence
- Sensitive

Information that requires protection is any information for which compromise threatens the security 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

Table 13: Information Classifications

Information that is classified IN CONFIDENCE or higher requires protection from unauthorised access during processing, transfer and while at rest. Endorsements should be used to differentiate Health, Staff and Commercial information types e.g. 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 e.g. Mental Health Information, Sexual Diseases, Abuse, etc.

Information that requires special handling will utilise 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 that is used in the Sector must be classified at a higher level. It is the responsibility of the originator (a person or organisation) to complete that classification evaluation.

Appendix C – Media Risk Assessment

The following are the various types of communication channels which could be used to transport personal health information and their relative risk, based on the risk of discovery in transmission or of disclosure at the receiving end. The higher the risk rating score, the higher the need for security controls.

Type	Media	Transmission Risk	Disclosure Risk		Risk Rating	Comments
	1-5: 1 = low, 5 = high	Probability	Probability	Impact		
Data	Internal LAN	1	2	2	6	
Data	Internet (encrypted/VPN)	1	1	4	8	
Data	Private Network	1	2	4	12	
Data	Store & Forward Messaging	2	2	3	12	DICOM email attachments
Data	Wireless Internal Network	1	2	4	12	secured to WPA2
Voice	Cellphone	1	2	4	12	
Voice	Internal PBX	2	2	3	12	
Data	Video-conferencing	1	2	5	15	multiple channels
Voice	cordless phone	3	2	3	15	
Voice	Landline (PSTN)	3	2	3	15	external
Data	Wireless remote access	2	2	4	16	E.g. EV-DO, WiMax, HSDPA/WCDMA
Storage	Fixed Disk storage	2	2	4	16	
Voice	Spoken voice	4	4	2	16	
Paper	Computer printout, labels	5	4	2	18	internal
Paper	Fax/Photocopy printout	5	4	2	18	internal
Paper	Handwritten note, forms	5	4	2	18	internal
Voice	Voice Messaging	2	4	3	18	
Data	Faxing	1	4	4	20	
Storage	Tapes	3	2	4	20	
Voice	Radio	4	3	3	21	
Data	Emailing	4	2	4	24	
Data	Internet (unencrypted)	3	3	4	24	
Voice	Dictation	3	3	4	24	
Paper	Courier/Registered	2	3	5	25	external

Type	Media	Transmission Risk	Disclosure Risk		Risk Rating	Comments
	1-5: 1 = low, 5 = high	Probability	Probability	Impact		
	post					
Storage	Removable hard disk	4	4	4	32	
Paper	Posted letter	3	4	5	35	external
Storage	Laptop	4	3	5	35	
Storage	Cellphone/PDA	4	3	5	35	
Data	Texting	4	5	4	36	Dependent on content and context of information
Data	Wireless Public Broadcast	5	5	4	40	802.11x unencrypted
Storage	CD, DVD, floppy, optical	4	4	5	40	
Storage	USB, Memory storage	4	4	5	40	

Table 14: Media Risk Assessment

Note that this table was derived from a consensus of committee member views, and is not based on independent research.