

Health Information Security Framework (HISF)

HISO 10029:2022

Graphical user interface, text, application

Description automatically generated

Citation: Te Whatu Ora – Health New Zealand. 2022. *HISO 10029:2022 Health Information Security Framework*. Wellington: Te Whatu Ora – Health New Zealand.

Published in December 2022 by Te Whatu Ora – Health New Zealand  
PO Box 793, Wellington 6140, New Zealand

ISBN 978-1-99-106707-4 (online)



This document is available at [tewhatuora.govt.nz](https://www.tewhatuora.govt.nz/)

|  |  |
| --- | --- |
| **CCBY** | This work is licensed under the Creative Commons Attribution 4.0 International licence. In essence, you are free to: share ie, copy and redistribute the material in any medium or format; adapt ie, remix, transform and build upon the material. You must give appropriate credit, provide a link to the licence and indicate if changes were made. |

Contents

[1 Introduction 4](#_Toc122434702)

[2 Scope 5](#_Toc122434703)

[3 Māori Co-design Objectives 6](#_Toc122434704)

[4 HISF Development 8](#_Toc122434705)

[5 HISF Framework 9](#_Toc122434706)

[5.1 HISF Obligations 11](#_Toc122434707)

[5.2 HISF Functional Processes 11](#_Toc122434708)

[5.3 Segmentation model 12](#_Toc122434709)

[5.4 Controls 15](#_Toc122434710)

[5.5 Cyber Security Requirements 16](#_Toc122434711)

[5.6 Guidance 18](#_Toc122434712)

[5.7 Tools and Templates 18](#_Toc122434713)

[6 References 19](#_Toc122434714)

[Appendix A – Glossary 21](#_Toc122434715)

List of Figures

[Figure 1: HISF Strategy Map 9](#_Toc122434716)

[Figure 2: Expected Outcomes 10](#_Toc122434717)

[Figure 3: HISF Foundational Building Blocks 11](#_Toc122434718)

[Figure 4: HISF Functional Processes 12](#_Toc122434719)

[Figure 5: Segmentation with risk characteristics 13](#_Toc122434720)

[Figure 6: HISF Maturity Assessment Scale 15](#_Toc122434721)

[Figure 7: Refreshed HISF Framework 16](#_Toc122434722)

[Figure 8: Five HISF functional processes with sub-categories 17](#_Toc122434723)

1. Introduction

The Health Information Security Framework (HISF), first published in September 2009 as HISO 10029.1-3 Health Information Security Framework, was updated as HISO 10029:2015 in December 2015. This updated version supersedes the HISO 10029:2015 framework.

In a rapidly changing security environment, the HISO 10029:2015 HISF is no longer considered fit for purpose. It is a challenging framework for health organisations to understand, adopt and use, particularly for smaller organisations which have limited access to information security expertise. In addition, it does not directly cater for Māori Health. The ever-changing information security landscape, including the increasing adoption of cloud-based solutions, was not adequately addressed in HISO 10029:2015. New and heightened cybersecurity risks are addressed in this updated framework.

The refreshed HISF is a set of materials including guidance documents, tools and templates that will be published to guide the New Zealand health and disability sector in the secure use and management of health information and information technology.

This refreshed version of the framework is designed for the reshaped operating environment introduced by the 2022 health reforms. The framework provides guidance and requirements that can be easily understood and requirements that can be easily met across the broad spectrum of health organisations and their industry partners.

HISO 10029:2022 also supports health system investments that will:

* improve system resilience by addressing issues resulting from technology infrastructure and systems that are out-of-support and no longer fit-for-purpose
* improve data and analytics capability across the health system so that equity issues can be targeted more effectively and to drive the development of new models of care
* improve information sharing between providers to facilitate greater collaboration and coordination of care
* empower New Zealanders to better manage their own health and wellbeing by providing more digital options for accessing care and information.

1. Scope

The HISF is concerned with the security of Health Information *wherever it may reside* including its storage and access.

Health information privacy is covered by the [Health Information Privacy Code](https://www.privacy.org.nz/privacy-act-2020/codes-of-practice/hipc2020/) 2020 and is not within the scope of this framework. Privacy is an outcome and relies on many mechanisms, only one of which is security.

The HISF assumes health information will be shared and restrictions on information sharing apply to patient personally identifiable information. All health information is treated as MEDICAL IN CONFIDENCE[[1]](#footnote-1) and given an equal level of protection unless otherwise classified.

1. Māori Co-design Objectives

The Māori co-design approach is developed to incorporate Te Tiriti obligations into the revised HISF. Below is Te Whatu Ora – Health New Zealand’s (Te Whatu Ora) expression of their obligations and how they will meet Te Tiriti obligation goals.

### Te Whatu Ora’s expression of Te Tiriti

The text of Te Tiriti, including the preamble and the three articles, along with the Ritenga Māori declaration, are the enduring foundation of our approach. Based on these foundations, we will strive to achieve the following four goals, each expressed in terms of mana.

* Mana whakahaere:   
  The effective and appropriate stewardship or kaitiakitanga over the health and disability system. This goes beyond the management of assets or resources.
* Mana motuhake:   
  Enabling the right for Māori to be Māori (Māori self-determination); to exercise their authority over their lives, and to live on Māori terms and according to Māori philosophies, values and practices including tikanga Māori.
* Mana tangata:   
  Achieving equity in health and disability outcomes for Māori across the life course and contributing to Māori wellness.
* Mana Māori:   
  Enabling Ritenga Māori (Māori customary rituals) which are framed by te ao Māori (the Māori world), enacted through tikanga Māori (Māori philosophy & customary practices) and encapsulated within mātauranga Māori (Māori knowledge).

### Te Whatu Ora’s approach to achieving these goals

The principles of Te Tiriti o Waitangi, as articulated by the Courts and the Waitangi Tribunal, provide the framework for how we will meet our obligations under Te Tiriti in our day-to-day work. The 2019 Hauora report recommends the following principles for the primary and community health care system. These principles that apply to our work are:

* Tino rangatiratanga:   
  The guarantee of tino rangatiratanga, which provides for Māori self-determination and mana motuhake in the design, delivery, and monitoring of health and disability services.
* Equity:   
  The principle of equity, which requires the Crown to commit to achieving equitable health outcomes for Māori.
* Active protection:   
  The principle of active protection, which requires the Crown to act, to the fullest extent practicable, to achieve equitable health outcomes for Māori. This includes ensuring that it, its agents, and its Treaty partner are well informed on the extent, and nature, of both Māori health outcomes and efforts to achieve Māori health equity.
* Options:   
  The principle of options, which requires the Crown to provide for and properly resource kaupapa Māori health and disability services. Furthermore, the Crown is obliged to ensure that all health and disability services are provided in a culturally appropriate way that recognises and supports the expression of hauora Māori models of care.
* Partnership:   
  The principle of partnership, which requires the Crown and Māori to work in partnership in the governance, design, delivery, and monitoring of health and disability services. Māori must be co-designers, with the Crown, of the primary health system for Māori.

1. HISF Development

The revised HISF shifts its focus from the existing ISO-centric model to incorporate a National Institute of Standards and Technology (NIST) Cybersecurity Framework-style model. The updated framework is considered a better fit that is more aligned to national and international standards.

An implementation guide for each segment will be agreed, published, and change management activities will commence.

1. HISF Framework

The HISO 10029:2022, HISF framework is an approach rather than a ‘yes’ and ‘no’ standard. It is more about how we think, which will be worked through as part of the developing Te Whatu Ora’s operating model. Health Information as referred to in this framework includes personal health information (PHI), patient personally identifiable information (PPII) and the implementation of general IT controls within the health service providers.

### HISF Strategy Map

The HISF strategy map is a single-page document that details Health and Disability Sector and user outcomes that the framework supports; the behaviour change levers the framework will employ; the foundations of a revised framework, and the supporting activities required to sustain it. The HISF strategy was developed through a co-design process with representatives from organisations across the health and disability sector. The HISF strategy is one pillar of the Te Whatu Ora’s three-year Cyber Security Uplift Programme (2022-2024). The programme is designed to uplift cyber security within three workstreams: Leadership Capability and Assurance, Sector Protect and Sector Detect, Respond Recover.

Text

Description automatically generated

Figure 1: HISF Strategy Map

The HISF strategy map supports the following outcomes:

|  |  |
| --- | --- |
| Outcomes sought | This could be observed by |
| * Improve health information security * Enable sharing personal health information to collaborated organisations * Build trust and confidence in the health sector’s ability to secure information | * Better incident response and more visible reporting * Improved patient wellbeing and clinical outcomes * Improved engagement and wide adoptions of HISF |

Figure 2: Expected Outcomes

Successful implementation of this framework will require the participants to:

* use the HISF as a key mechanism for assessing and improving information security maturity, and manage the organisation’s risk profile
* acknowledge their obligations, assess themselves and share their level of maturity allowing Te Whatu Ora and other key stakeholders such as Primary and Secondary & Community Health Care, to measure and manage security uplift.

The HISF’s development pathway consists of the following seven foundational building blocks:

|  |  |
| --- | --- |
| Building Block | Description |
| Obligations | To uphold and maintain adherence to the wairua or spirit and intent of the information security principles, in all endeavors to achieve and maintain health information security. |
| Functional Processes | Provide strategic guidance on how an organisation can protect their systems and data from cyber threats. |
| Segmentation Model | Health sector segments so the HISF is tailored appropriately to different types of organisations and audiences. |
| Controls | Safeguards or countermeasure prescribed for an information system, or an organisation designed to protect the confidentiality, integrity, and availability of the system and its information. |
| Requirements | Plain ENGLISH descriptions of what information security practices are required and are the ore of the framework for maturity assessment. |
| Guidance | The activities the organisation need to implement to meet the requirement. |
| Tools and Templates | Segment-specific toolkits and templates will be available for reference. |

Figure 3: HISF Foundational Building Blocks

To succeed, the HISF needs to *Motivate, Build Capability and Remove Barriers for health care providers*. The four implementation support elements underpin these foundational building blocks. Namely, *marketing & user support, monitoring & measurement, maintenance & governance, and funding*.

* 1. HISF Obligations

All organisations that collect, process or store personal health information related to New Zealanders have the following obligations:

* **Te Tiriti o Waitangi**  
  ensure the application of the framework progresses the health and well-being of Māori, does not place undue burden on the Māori health sector and that Māori data is collected, stored, and transferred in ways that enable and reinforces the capacity of Māori to exercise kaitiakitanga over Māori data.
* **Confidentiality**  
  ensure personal health information is accessible to those authorised for access.
* **Integrity**  
  ensure the safeguarding, the accuracy and completeness of information, its handling and processing.
* **Availability**  
  ensure authorised users have access to personal health information when required.
  1. HISF Functional Processes

There are five HISF functional processes (Plan, Identify, Protect, Detect, and Respond) that support the four HISF obligations as described in the previous section.

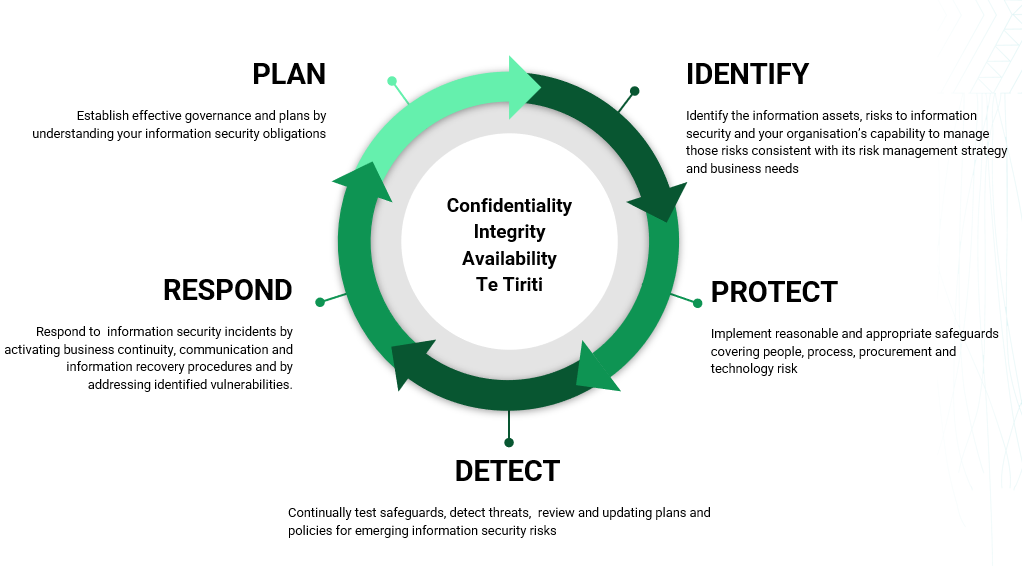


Figure 4: HISF Functional Processes

The five functional processes are a high-level grouping of the elements for HISF that represent the primary pillars for a successful and holistic cybersecurity and have been adapted from the NIST Cybersecurity Framework[[2]](#footnote-2).

Overall, the functional processes are designed to reinforce the continuous nature of organisational behaviour and practice with respect to information security as well as:

* describe required organisational capabilities to manage information security
* be understandable to everyone
* be applicable to any size or type of organisation and their information security risk profile
* span both prevention and response to vulnerabilities and threats.
  1. Segmentation model

The segmentation model conceptualises types of health sector organisations that share similar information security risk profiles and thus similar requirements for managing information security risk.

The purpose of the segmentation model is to make it easier for health care providers to recognise the nature of information security risk they face and to easily find the guidance and controls most appropriate to them.

The model recognises diversity and the broad spectrum of organisations that comprise the New Zealand health and disability sector with varying risk profiles (ie, likelihood of risks and potential impacts/ consequences).

* + 1. Common risk characteristics

Based on the co-design approach, the risk characteristics below are identified as common across each segment. Controls are designed based on the implementation capabilities and areas of expertise across each segment (eg, Government Agencies vs NGOs).

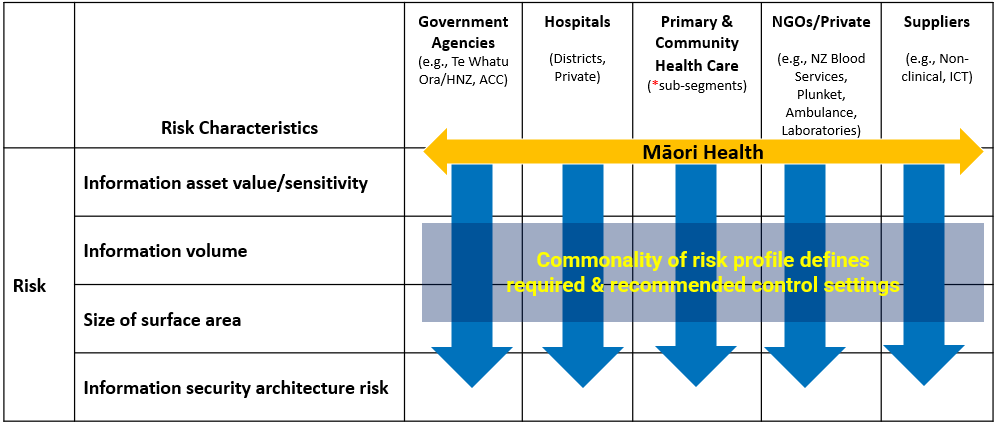


Figure 5: Segmentation with risk characteristics

\* Primary & Community Health Care sub-segments: Micro to Small & Medium to Large providers. For more details, refer to HISO 10029.2:2023 HISF Guidance for Primary & Community Health Care.

Note that the key health segments are grouped vertically. Definitions of the horizontal grouping of risk characteristics are as follows:

* **Information asset value/sensitivity**  
  is the nature of the personal health information captured, processed, stored, or transmitted by an organisation and how valuable it may be considered by the individuals who provide it to an organisation.
* **Information volume**  
  is the absolute quantity of personal health information captured, processed, stored, or transmitted by an organisation. This would include the total number of individual records held and the number of health information data points for each individual.
* **Size of surface area**  
  this relates to the number of endpoints (eg, devices, APIs, servers, systems, and platforms) that an organisation is responsible for managing and therefore securing.
* **Information security architecture risk**  
  this relates to the nature of the information systems that an organisation is responsible for securing (eg, on-premises infrastructure, cloud-based platforms and software as a service and use of third-party vendors for services and security).
  + 1. Segmentation and maturity

The maturity of the practices and behaviours of health and disability organisations in regard to the functional processes described by the HISF varies both between segments and within segments.

The HISF recognises varying levels of maturity across the health and disability sector in two ways:

* Providing different guidance and requirements for organisations in each segment. Some segments will have a comprehensive implementation guide, while others will have a simplified guide based on the nature of the audience. The guidance will contain ideal practices that are articulated by the combination of requirements and controls defined under each of the five functional processes for organisations in a specific segment.
* Providing a maturity assessment model to allow organisations to assess maturity against the guidance and requirements for organisations in each segment.

The HISF maturity assessment model uses a rating scale to assess the extent to which requirements or security controls are implemented. A self-assessment at an organisational level against each requirement per segment will be included with the HISF in future. The maturity assessment below containing a scale of 1 to 5 is consistent with AS/NZS 33004:2016.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HISF Maturity Assessment Scale | | | | |
| **1-None** | **2-Emerging** | **3-Partially Applied** | **4-Maturing** | **5-Embedded** |
| No understanding of this cyber security concept and/or no control is in place to support the requirement. | Not formally in place but some form of controls exists to support the requirement. These are not documented, and/or there are significant gaps in their application to areas or systems. | Controls exist and are applied, but they are not thoroughly formalised or documented, and/or they are not consistently applied to all functional areas or systems. | Controls exist and are formally documented. They are regularly applied across most functional areas and systems. There is some monitoring of control effectiveness and attempts at control improvement. | Robust controls are in place with documentation. They cover all functional areas and systems and are periodically reviewed for monitoring and continuous improvement. The requirement is completely met. |

Figure 6: HISF Maturity Assessment Scale

* 1. Controls

Controls are also safeguards or countermeasures to detect, avoid, mitigate, or reduce organisational, people, physical and technology risks. They are also risk reduction measures with associated compliance requirements.

### HISF mappings to control catalogues

The revised HISF does not create a duplicate of relevant ISO standards. Rather it links directly to the relevant and dominant controls catalogues of the NZISM, Center for Internet Security (CIS), Cloud Controls Matrix (CSA), ISO 27002, ISO 27799, Secure Controls Framework, HIPAA, PSR and CERT NZ Top Ten.

The refreshed HISF is a medium through which the guidance to organisations about relevant controls for each is tailored based on their risk segment and maturity levels.

The rationale for mapping the proposed maturity requirements to these control catalogues is as follows:

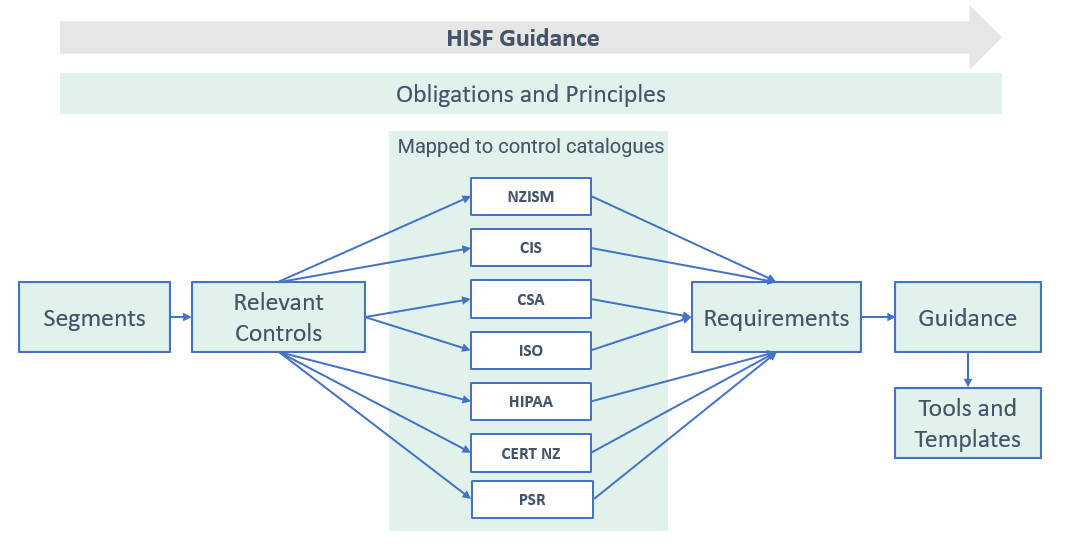


Figure 7: Refreshed HISF Framework

The ‘Obligations’ and ‘Principles’ of the HISF are overarching and apply to all health and disability sector organisations. ‘Segments’ defined within the HISF allow for ‘Requirements’ to be tailored to varying levels of information security risk across segments. The requirements may change in response to changes in the threat environment and evolving maturity of a segment.

The control catalogues describe specific safeguards that can be implemented to meet HISF Requirements. The control catalogues described in Figure 7 have been mapped to the Requirements for each Segment. An organisation can choose the relevant guidance for it to meet the specified Requirements and its overall HISF obligations. As control catalogues are updated regularly, these are mapped rather than replicated within the HISF. The mapping within the HISF will be updated periodically.

The ‘Guidance’ section of the HISF provide recommended capabilities and practices for organisations to meet the specified Requirements and overall HISF obligations. The HISF guidance may change periodically as a living document planned to reflect the updated guidance. To help the relevant segments based on their capabilities, standard operating procedures and workflows will be provided as part of ‘Tools and Templates’.

* 1. Cyber Security Requirements

The functional processes are underpinned by **cyber security requirements**. Requirements are high level statements which act as a checklist for the organisation to determine their HISF compliance status. They are also the statements which also provide a foundation for a defence-in-depth protection.

The requirements are grouped according to the five HISF functional processes with sub-categories as defined below. The sub-categories are an organising construct to group the more detailed requirements into areas of common practice and capability.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PLAN | IDENTIFY | PROTECT | DETECT | RESPOND |
| Acknowledge your obligations and put in place effective governance and plans to protect the security of health information. | Identify your information assets and understand the risks to information security and your organisation’s capability to manage those risks (consistent with its risk management strategy and business needs) | Implement reasonable and appropriate safeguards covering people, process, procurement and technology risk | Continually test safeguards, detect threats, review and updating plans and policies for emerging information security risks | Respond to information security incidents by activating business continuity, communication and information recovery procedures and by addressing identified vulnerabilities. |
| **Establish governance** | **Identify risk** | **People risk** | **Test safeguards** | **Activate plans** |
| **Plans & Policies in place** | **Determine capability** | **Process risk** | **Review and update** | **Address vulnerabilities** |
|  |  | **Technology risk** | **Monitor for events** | **Recover** |
|  |  | **Procurement risk** |

Figure 8: Five HISF functional processes with sub-categories

The complete set of *proposed* requirements can be found in respective guidance documents for each segment.

The requirements presented in the respective guidance documents represent a common set of activities for managing cybersecurity risk. While it is not exhaustive, it is extensible, allowing organisations, sectors, and other entities to use subcategories and informative references that are cost-effective and efficient and that enable them to manage their cybersecurity risks.

* 1. Guidance

Guidance indicates the detailed level of implementation activities which the organisation needs to achieve control effectiveness. The implementation details are to be followed as appropriate to the organisation and system under consideration.

* 1. Tools and Templates

A separate set of documents which are a combination of checklists and guides will be provided to the sector entities where there is limited or no documentation available to assist with the implementation activities of HISF. These documents could be tailored to fit for purpose based on the needs and requirements.

They also consist of a self-completion questionnaire using appropriate questions for organisations in each segment. Evidence confirming the implementation for each requirement may be used for reporting and planning of any cyber security initiatives.

1. References

When looking at each of the references below, ensure that the most recent version is identified and used:

* [Center for Internet Security (CIS):](https://www.cisecurity.org/controls/v8)  
  Are designed to support the NIST framework developed in the USA and seen by many local information security practitioners to provide up-to-date guidance on international best practice.
* [CERT NZ Top Ten:](https://www.cert.govt.nz/it-specialists/critical-controls/10-critical-controls/)  
  Intended to help organisations decide what to spend the time and money on based on the assessment of 10 most critical controls.
* [Cloud Security Alliance (CSA) Cloud Controls Matrix:](https://cloudsecurityalliance.org/research/cloud-controls-matrix/)  
  The Cloud Security Alliance controls are regarded as best-practice from organisations that have adopted as-a-service computing. Given the trajectory for the adoption of cloud computing services will continue to grow in the NZ health sector, the CSA controls provide international best-practice for controls in cloud computing environments.
* [Health Insurance Portability and Accountability Act (HIPAA) (US):](https://www.cdc.gov/phlp/publications/topic/hipaa.html)  
  US based federal law that required the creation of national standards (HIPAA Security Rule) to protect sensitive patient health information from being disclosed without the patient’s consent or knowledge.
* [ISO 27001 Information Security Management Standard:](https://www.iso.org/isoiec-27001-information-security.html)  
  An information Security Standard that provides requirements for an information security management system (ISMS).
* [ISO 27002 Information Technology – Security Techniques – Code of practice for information security controls:](https://www.iso.org/standard/75652.html)  
  An Information Security Standard that provides guidance on implementing ISO 27001:2022 Information Security Management System (ISMS).
* [ISO 27799 Health informatics – Information Security Management in health using ISO/IEC 27002:](https://www.iso.org/standard/62777.html)  
  The Health information specific version of the ISO 27002:2013 standard upon which the HISF was initially based.
* [New Zealand Information Security Manual (NZISM):](https://www.nzism.gcsb.govt.nz/ism-document/)  
  The dominant New Zealand information security framework provides the assurance of providing best-practice controls in a local context and reflects internationally accepted standards and controls.
* [Protective Security Requirements (PSR):](https://www.protectivesecurity.govt.nz/)  
  Outlines the New Zealand government’s expectations for security governance and for personnel, information and physical security.
* [Secure Controls Framework (SCF):](https://www.securecontrolsframework.com/)  
  Contains a collection of controls catalogues compiled by an organisation called the Secure Controls Framework Council, LLC.
* [UK National Health Service assertions:](https://www.dsptoolkit.nhs.uk/News)  
  A UK based Data Security and Protection Toolkit is an online self -assessment tool that allows organisations to measure their performance against the National Data guardian’s 10 data security standards. It comprises of several assertions and evidence items.
* [US National Institute of Standards and Technology (NIST):](https://www.nist.gov/cyberframework)   
  A US based framework for improving critical infrastructure cyber security.

### New Zealand Legislation

The following Acts of Parliament and Regulations have specific relevance to this standard. Readers must consider other Acts and Regulations and any amendments that are relevant to their own organisation when implementing or using this standard:

* Crimes Act 1961
* Electronic Transactions Act 2002
* Health Act 1956
* Health and Disability Commissioner (Code of Health and Disability Services Consumers’ Rights) Regulations 1996
* Health Information Privacy Code 2020
* Health Practitioners Competence Assurance Act 2003
* Injury Prevention, Rehabilitation, and Compensation Act 2001
* Mental Health (Compulsory Assessment and Treatment) Act 1992
* Pae Ora (Healthy Futures) Act 2022
* Public Records Act 2005
* Privacy Act 2020

# Appendix A – Glossary

|  |  |
| --- | --- |
| Term | Definition |
| Health Information / Personal Health Information | Health information is defined, broadly, in clause 4 of the Health Information Privacy Code 1994 and includes any information about the health of an identifiable individual, or any health or disability services provided to him or her. It also includes any information collected incidentally to providing services, such as appointment times and demographic data. It does not include anonymous data as it must be about an identifiable individual.  This document focuses on the sharing of health information as defined above. For clarification, we have referred to any information about the health of an identifiable individual as personal health information. |
| Information Security Architecture | A description of the structure and behaviour for an enterprise's security processes, information security systems, personnel and organisational sub-units, showing their alignment with the enterprise's mission and strategic plans. |
| NGO | An NGO (Non-government organisation) is a non-profit, independent, community organisation that is not affiliated with central or local government, although they may receive financial and/or other support from the Government. |
| Personnel | Includes permanent, fixed term and temporary staff, contractors, consultants, volunteers, locums, and suppliers. |
| PSR | Protective Security Requirements (PSR) outlines the Government's expectations for managing personnel, physical and information security. As part of this framework, the mapping to the PSR does not have a complete cover but is noted as per HISF requirements.  Note that this applies to selected organisations only. We recommend checking with your respective PSR obligations before cross referencing. |
| Risk | A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of:   * The adverse impacts that would arise if the circumstance or event occurs; and * The likelihood of occurrence. |
| Supplier | Organisation or an individual that enters into an agreement with the acquirer for the supply of a product or service. This includes all suppliers in the supply chain, developers or manufacturers of systems, system components, or system services; systems integrators; suppliers; product resellers; and third-party partners. |
| User | A user is a person issued with a unique user ID who is authorised to use a computer system. |

1. The New Zealand government defines ‘IN CONFIDENCE’ as information that if released “would be likely to prejudice the maintenance of law and order, impede the effective conduct of government in New Zealand or affect adversely the privacy of its citizens”. Department of Prime Minister and Cabinet, Cabinet Office Circular CO (08) 01 <http://www.dpmc.govt.nz/cabinet/circulars/co08/1>

   From a practitioner viewpoint, IN CONFIDENCE mirrors doctor patient confidentiality and means that a person’s health information won’t be disclosed unless consented to or authorised by that person (eg, through a privacy fact sheet), by another authorised person, under statutory authority or by a legal instrument (eg, an Approved Information Sharing Agreement). [↑](#footnote-ref-1)
2. <https://www.nist.gov/cyberframework> [↑](#footnote-ref-2)