Frequently Asked Questions (FAQ)

HISF for suppliers

HISO 10029.4:2025/ Released April 2025

Introduction

This document answers questions which are often posed by suppliers in the New Zealand health and disability sector who supply services or products to Health New Zealand. These questions relate to the use of the Health Information Security Framework (HISF), which has relevant content available on the HISO website: HISO 10029.4:2025 HISF Guidance for Suppliers and the Health New Zealand Cyber Hub.

Questions have been grouped into topics of privacy, data, alternative security frameworks and questions relating to the Health New Zealand Cyber Risk Assurance processes.

Feedback on this document is highly encouraged to ensure its continued relevance and effectiveness. Users are invited to submit comments, suggestions, and any identified areas for improvement to CyberAssurance@TeWhatuOra.govt.nz. This feedback will be used to update and refine the document, ensuring it remains a valuable resource for suppliers in the health and disability sector working to protect sensitive health information.

Privacy

01 – How should we go about officially reporting a breach of privacy or a security incident?

In New Zealand, there are specific steps to follow when reporting a privacy breach. Details can be found on the Privacy Commissioner's website.

For security incidents specifically, refer to guidelines like those provided by the New Zealand government for Protective Security Requirements or submit a report to CERTNZ.

A service provider or supplier of Health New Zealand should notify their HNZ contact if they suspect or have had a data breach.

Tools or Links:	Office of the Privacy Commissioner | Privacy breaches Reporting incidents and conducting security investigations | Protective Security Requirements Report an incident | CERT NZ

02 – What are the breach notification requirements in the case that confidential information or Health information (PHI) is breached?

When confidential health information (PHI) is breached, the following breach notification requirements apply:

- **Notification to the Privacy Commissioner**: If the breach is likely to cause serious harm, notify the Privacy Commissioner as soon as practicable.
- **Notification to affected individuals**: Inform affected individuals directly unless it is not reasonably practicable, in which case public notice may be given.
- **Considerations for PHI**: Given the sensitive nature of health information, organisations must consider the potential harm and take steps to mitigate risks.

Tools or Links:	Office of the Privacy Commissioner | Breach Management

03 - Who can access and view patient records (PHI)? What are the guidelines around this?

Access to patient records (PHI) is typically restricted to authorized personnel who need the information to perform their duties. Guidelines include:

- **Need-to-know principle**: Only those with a legitimate need should access PHI.
- **Authorisation**: Access must be authorized and controlled through appropriate access controls and permissions.
- **Confidentiality**: PHI must be handled confidentially to protect patient privacy.

- **Security measures**: Implement robust security measures to prevent unauthorized access, such as encryption and secure authentication.

Tools or Links:	**Office of the Privacy Commissioner | Health Information Privacy Code 2020**

04 - What are the key differences between security requirements and privacy requirements in relation to the HISF Suppliers Framework?

Some key differences between security and privacy requirements are:

	Security	**Privacy**
Focus	Protecting systems and data from unauthorized access, use, disclosure, disruption, modification, or destruction.	Protecting personal information from unauthorized access, disclosure, alteration, loss, or destruction.
Scope	Includes confidentiality, integrity, availability, threat protection, and monitoring.	Focuses on the handling of personal information to prevent breaches and ensure compliance with privacy laws.
Regulations and Standards	HISF does not have a legislative mandate, however it includes requirements that map to the NZISM and standards published by HISO.	Follows the Privacy Act 2020 and related regulations for breach notification and individual rights.

Tools or Links:	Privacy Act 2020 No 31 (as at 26 January 2025), Public Act Contents – New Zealand Legislation About the NZISM | New Zealand Information Security Manual Health Information Standards Organisation (HISO) – Health New Zealand | Te Whatu Ora

Data

05 - Where can Health Information (PHI) be sent or stored? Geographically, what are my obligations?

Health Information (PHI) can be stored within New Zealand or overseas, but there are specific obligations to consider:

- **Data Sovereignty**: While there is no strict prohibition on storing PHI outside New Zealand, organizations must ensure that any offshore storage complies with New Zealand privacy laws and standards, such as the Privacy Act 2020. This includes ensuring that the data is protected to the same standards as in New Zealand.
- **Cloud Services**: If using cloud services, ensure they meet New Zealand's data security standards. The Ministry of Health encourages the use of cloud platforms designed for data science to manage national data collections4.
- **Geographical Obligations**: Organizations must ensure that PHI is stored securely, regardless of location, and that access is restricted to authorized personnel. This includes implementing robust security measures like encryption and access controls.

Tools or Links:	Office of the Privacy Commissioner | Principle 12 - Disclosure outside New Zealand Cloud services | NZ Digital government

06 - What are the data retention requirements for Health information (PHI)? What about exceptions?

Data retention requirements for PHI in New Zealand generally follow these guidelines:

- **Standard Retention**: Health data related to an identifiable individual should be stored for at least 10 years, as required by New Zealand law.
- **Exceptions**: Exceptions may apply based on specific legal or regulatory requirements. For example, if data is no longer needed for its original purpose, it should be disposed of securely unless there are legal reasons to retain it.
- **Data Governance**: Robust data governance is crucial to ensure that data is not stored longer than necessary and that it is managed throughout its lifecycle.

Tools or Links:	Health (Retention of Health Information) Regulations 1996 (SR 1996/343) (as at 01 July 2022) – New Zealand Legislation

07 – What are the levels of data classification for Health Information (PHI)? Is there best practise for how to go about data classification based on roles and responsibilities?

The levels of data classification for PHI in New Zealand are primarily guided the Protective Security Requirements (PSR):

- **Classification Levels**: All personal health information is treated as **MEDICAL IN CONFIDENCE** unless otherwise classified.
- **Best Practice for ensuring appropriate security for specific data classification**:
- **Role-Based Access**: Implement role-based access controls to ensure that only authorized personnel can access PHI.
- **Need-to-Know Principle**: Apply the need-to-know principle to limit access to sensitive information.
- **Clear Policies**: Establish clear policies and procedures for data classification and access, ensuring that all staff understand their roles and responsibilities in managing PHI.
- **Regular Review**: Regularly review and update classification and access controls to ensure they remain appropriate and effective.

Tools or Links:	Classification system | Protective Security Requirements

Frameworks and Guidance

08 – I am aligned with NIST and have ISO27001 Certification, what does this mean in the context of HISF?

Being aligned with NIST and/or holding ISO 27001 certification in the context of the Health Information Security Framework (HISF) means that your organisation has a robust foundation for managing information security and you may already be meeting HISF requirements:

- HISF has been mapped to the Secure Control Framework (SCF), as has the NST CSF 2.0 and ISO 27001.
- The SCF is a meta-framework (framework of frameworks) that maps to more than 100 cybersecurity and privacy-related laws, regulations and industry. This Open-Source project has a library of more than 1200 controls and HISF requirements have been mapped to a sub-set of these controls.
- This means you can download (at no cost) the crosswalk matrix and select the controls for the framework that you have certified to (e.g. NIST CSF 2.0 or ISO 27001) and identify any gaps that you need to address to conform with all the HISF requirements.

Tools or Links:	Secure Controls Framework (SCF) Download

09 – What are some information policies and procedures that may be beneficial for my organisation to have?

Beneficial information policies and procedures for your organization include:

- **Acceptable Use Policy**: Define organisation's expectations for staff or contractors to access, store or use digital assets and information.
- **Data Access Policy**: Define who can access health information and under what conditions, ensuring compliance with privacy laws.
- **Incident Response Plan**: Establish procedures for responding to security incidents, including breach notification and containment.
- **Data Retention and Disposal Policy**: Outline how long data should be kept and how it should be securely disposed of.
- **Third-Party Risk Management Policy**: Specify how third-party vendors are assessed and managed to mitigate risks.
- **Training and Awareness Program**: Regularly educate staff on security best practices and policies to foster a security-conscious culture.

Tools or Links:	Information Security Policy Templates | SANS Institute

10 – I am an MSP – what does a third-party security risk assessment mean for me?

As a Managed Service Provider (MSP), third-party security risk assessments are crucial for managing risks associated with your services and ensuring the security of your clients' data:

- **Risk Assessment Process**: Conduct thorough assessments of your own security posture and that of any third-party vendors you engage. This includes evaluating their access to sensitive data, security controls, and compliance with relevant standards.
- **Mitigation Strategies**: Develop and implement strategies to mitigate identified risks, such as contractual requirements for security standards, regular audits, and incident response plans.
- **Ongoing Monitoring**: Regularly monitor and reassess third-party risks to ensure that your security posture remains robust and aligned with evolving threats and standards.

Tools or Links:	Office of the Privacy Commissioner | Working with third-party providers: understanding your privacy responsibilities Supply Chain | New Zealand Information Security Manual

11 - Why is cyber security important to HNZ?

Cyber security is crucial for Health New Zealand (HNZ) because it directly impacts the safety and efficiency of healthcare services. Moreover, the healthcare sector handles sensitive personal health information, making robust cyber security essential to maintain public trust and comply with privacy regulations like the Health Information Privacy Code 2020.

Some of the main drivers for building and maintaining a robust and resilient cyber posture:

- The health sector remains one of the most attacked sectors not just in New Zealand but globally and incident trends suggest attacks on healthcare in NZ will increase exponentially. Cyber incidents can significantly disrupt an organisation's ability to operate, and some organisations are unable to recover at all.
- New Zealand legislation, the Privacy Act 2020 sets requirements regarding security safeguards referred to as Information privacy principle 5
- Commercial agreements like the PHO Service Agreement, Data Sharing Agreements, Remote Access Agreements etc
- Professional Duty of Care – Professional duty of care in cybersecurity obligates individuals and organisations to act with reasonable prudence in implementing basic critical cyber controls. This means taking necessary steps to protect systems and data from foreseeable threats, aligning with industry standards such as HISF and legal obligations to prevent a breach.

Tools or Links:	Office of the Privacy Commissioner | Working with third-party providers: understanding your privacy responsibilities Supply Chain | New Zealand Information Security Manual

12 – What are HNZ's expectations from its third parties?

HNZ expects third parties to align and conform with the HISF. The requirements in HISF have a collection of controls based on the risk classification of the services and/or information that the third party will access. In general, HNZ expects:

- **Compliance with Regulations:** Vendors must comply with relevant laws and regulations, such as the Privacy Act 2020 and the Health Information Privacy Code 2020
- **Risk Management Approach:** HNZ expects all third parties to maintain a robust risk management practice. This includes proactively identifying potential risks that could impact our collaboration or shared information and implementing appropriate measures to treat and mitigate those risks effectively.
- **Cyber Security Measures:** Implementing robust cyber security measures to protect health information.
- **Transparency and Communication:** Open communication about any security incidents or changes that could impact their services.
- **Continuous Improvement:** Regularly updating systems and processes to address emerging cyber threats and maintain the integrity of health data.

Tools or Links:	HISO 10029.4: 2023-HISF Guidance for Suppliers

13 – How does the new information sharing standard relate to HNZ and HISF?	
The new government information sharing standard requires all government agencies to ensure third parties handling sensitive information comply with the Privacy Act and all relevant legislation. From a cyber security perspective, Health New Zealand will assess confidentiality, integrity, and availability of applicable data, systems and services using the Health Information Security Framework (HISF). The adoption, alignment, and maturity with respect to the HISF will serve as the principal metrics for evaluating the cyber posture of all third parties.	
Tools or Links:	Information sharing | NZ Digital Government HISO 10029.4: 2023-HISF Guidance for Suppliers

Health New Zealand
Te Whatu Ora