SmartSuite

Framework / Cybersecurity / Other

HISO 10029:2022 Health Information Security Framework (HISF)

HISO 10029:2022 is Health New Zealand's Health Information Security Framework: four obligations, five functional processes and segment-based requirements for protecting health information.



What it is

The Health Information Security Framework (HISF), published as HISO 10029:2022 by Health New Zealand | Te Whatu Ora in December 2022, is the New Zealand health sector's national cyber security framework. It guides every organization that collects, processes or stores personal health information, from hospitals and general practices to software suppliers. It has no legislative mandate; Health New Zealand's FAQ for suppliers adds that the agency expects third parties to conform.

The core document is an umbrella. It sets a strategy map, four obligations (Te Tiriti o Waitangi, confidentiality, integrity and availability), five functional processes (Plan, Identify, Protect, Detect and Respond) and a segmentation model.

At a glance

PUBLISHER Health New Zealand | Te Whatu Ora (HISO)	TYPE Framework	VERSION HISO 10029:2022 (core framework; segment guidance 10029.1 to 10029.4 published separately)
EFFECTIVE December 2022	DOMAIN Cybersecurity	FAMILY Other
REGION New Zealand	INDUSTRY Healthcare & Life Sciences	ADOPTION MODEL Industry Requirement
IMPLEMENTATION COMPLEXITY Medium		

Source: healthnz.govt.nz/health-professionals/guidance-standards/topic/digital-technologies/cyber-security-hub/health-security-frameworks

Why it matters

- **Shared obligations** Section 5.1 applies Te Tiriti o Waitangi, confidentiality, integrity and availability to every organization handling personal health information, including Māori data and the exercise of kaitiakitanga over it.
- **Requirements sized to the organization** The section 5.3 segmentation model groups organizations by information value, volume, surface area and architecture risk, so a small practice and a hospital do not carry the same requirements.
- **A scale for reporting maturity** Section 5.3.2 rates each requirement from 1 (None) to 5 (Embedded), giving organizations and Health New Zealand a common measure of progress.
- **Mapped, not duplicated** Section 5.4 maps requirements to NZISM, CIS, the CSA Cloud Controls Matrix, ISO 27002, ISO 27799, HIPAA, PSR and the CERT NZ Top Ten instead of reproducing them, and the mappings are updated periodically.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports NZ HISF 2022

Segment Requirement Library

Load the requirements from the guidance for your segment, hospital, micro to small, medium to large or supplier, as records with owners, status and linked evidence.

Maturity Scoring

Record the 1 to 5 maturity rating for each requirement with its supporting evidence and review date, so a self-assessment is a report rather than a spreadsheet.

Obligations Register

Track the four section 5.1 obligations as controls with owners, including decisions about Māori data and kaitiakitanga.

Five-Process Risk Register

Link risks and treatments to Plan, Identify, Protect, Detect and Respond, including people, process, technology and procurement risk, in Cyber & IT Risk.

Control Catalog Mappings

Map each requirement to the NZISM, CIS or ISO 27002 control that meets it, so one control set answers several assessors.

Supplier and Incident Records

Track supplier assurance in Third Party Risk Management and log security incidents with response actions and lessons learned, with dashboards for leadership reporting.

Common framework mappings

HIPAA (NIST SP 800-66 Rev. 2) · HITRUST CSF v11.5 · ISO 27001:2022 · ISO 27002:2022 · NIST CSF 2.0 · NIST 800-53 Rev.5 · NZISM 3.6 · PCI DSS 4.0.1

Official resources

New Zealand Health Information Security Framework (HISF) 2022

Defines security controls and privacy measures for safeguarding health information in New Zealand.

healthnz.govt.nz/health-professionals/guidance-standards/topic/digital-technologies/cyber-security-hub/health-security-frameworks

HISO approved health information standards (information governance)

Health New Zealand's list of approved HISO standards, including HISO 10029:2022 and its segment guidance documents.

healthnz.govt.nz/health-professionals/guidance-standards/topic/data-and-standards/health-information-standards/approved-health-information-standards/information-governance

HISF cyber security resources for suppliers

Health New Zealand's supplier page: the HISO 10029.4 guidance for suppliers and the supplier self-assessment resources.

healthnz.govt.nz/health-professionals/guidance-standards/topic/digital-technologies/cyber-security-hub/cyber-security-resources-for-suppliers

New Zealand Privacy Act 2020 (Office of the Privacy Commissioner)

The information privacy principles the HISF sits under, as published by the Office of the Privacy Commissioner.

privacy.org.nz/privacy-principles

Frequently asked questions

What is HISO 10029:2022, the Health Information Security Framework?

It is the New Zealand health sector's national cyber security framework, released in December 2022 by Health New Zealand | Te Whatu Ora. Section 1 describes it as a set of materials that guide the secure use and management of health information and information technology. It follows the 2015 second edition and is based on the NIST Cybersecurity Framework rather than ISO (section 3).

Is HISF mandatory in New Zealand?

No statute or regulation requires HISF. Health New Zealand's FAQ for suppliers says it has no legislative mandate, yet the agency expects third parties to conform and plans to treat their alignment and maturity as the main measure of cyber posture. Section 5 of the framework calls itself an approach to cyber security rather than a yes-or-no standard. Privacy is handled outside it, under the Health Information Privacy Code 2020.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What are HISF's obligations and functional processes?

Section 5.1 sets four obligations: Te Tiriti o Waitangi, confidentiality, integrity and availability. Section 5.2 defines five functional processes, adapted from the NIST Cybersecurity Framework: Plan, Identify, Protect, Detect and Respond. Section 5.5 groups the requirements under them, with sub-categories such as governance, risk, people, process, technology, procurement, testing and recovery.

How does an organization know which HISF guidance applies?

Section 5.3 sets up a segmentation model based on information value, volume, surface area and architecture risk. Health New Zealand publishes guidance for hospitals (HISO 10029.1:2023), micro to small organizations (10029.2:2023), medium to large organizations (10029.3:2023) and suppliers (10029.4:2025). Its cyber hub gives each segment's criteria, such as up to 25 staff for micro to small organizations.

How does the HISF maturity scale work?

Section 5.3.2 rates how far each requirement or control is implemented on a scale of 1 to 5: None, Emerging, Partially Applied, Maturing and Embedded. Level 5 means the requirement is completely met, with controls documented, covering all functional areas and systems, and periodically reviewed. Section 5.7 adds a self-completion questionnaire for each segment, and evidence for each requirement can support reporting.

License included / downloadable: Yes HISO 10029:2022 is published free by Health New Zealand | Te Whatu Ora under the Creative Commons Attribution 4.0 International license, and the platform links to the official document.

Full framework page and mappings: smartsuite.com/frameworks/new-zealand-hisf-2022-health-information-security-framework