SmartSuite

Framework / Data Protection & Privacy / Other

New Zealand Health Information Security Framework (HISF) 2022

HISF 2022 is a New Zealand framework guiding health organizations to protect patient data and manage cybersecurity and privacy risks.

Te Whatu Ora
Health New Zealand

What it is

The New Zealand Health Information Security Framework (HISF) 2022 is a national cybersecurity and risk management framework that enables healthcare organizations to safeguard health information and maintain compliance with regulatory requirements. HISF 2022 establishes security controls and privacy measures designed to protect sensitive patient data and ensure the resilience of health sector information systems.

Developed and published by Te Whatu Ora – Health New Zealand, the HISF 2022 serves healthcare providers, government agencies, and IT service partners responsible for handling health information. The framework covers areas such as risk assessment, cybersecurity controls, incident response, privacy governance, and operational resilience, aligning with local laws and broader global standards.

At a glance

PUBLISHER Health New Zealand | Te Whatu Ora	TYPE Framework	VERSION 2022
EFFECTIVE 23 December 2022	DOMAIN Data Protection & Privacy	FAMILY Other
REGION New Zealand	INDUSTRY Healthcare & Life Sciences	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

Source: https://www.tewhatuora.govt.nz

Why it matters

- **Strengthen information security governance** Establish clear accountability and oversight for safeguarding patient data and managing information security risks across healthcare operations.
- **Enhance regulatory and legal alignment** Support adherence to New Zealand health information laws and align data protection practices with both local and international regulatory requirements.
- **Improve incident response capabilities** Enable prompt detection, assessment, and mitigation of security incidents affecting health sector systems and sensitive data.
- **Promote operational resilience** Reduce downtime and maintain critical healthcare services through robust risk management and continuity planning measures.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports NZ HISF 2022

Health Information Security Control Framework

Structure HISF control domains with ownership, scope, and implementation tracking.

Clinical Data Protection and Privacy Controls

Manage safeguards for patient data confidentiality, integrity, and secure access.

Risk Assessment and Security Governance

Track healthcare-specific risks, mitigation actions, and governance processes.

Access Control and Identity Management

Manage user access, authentication, and role-based permissions across clinical systems.

Health Data Breach Monitoring and Response

Monitor security incidents and manage response workflows for health data breaches.

HISF Compliance Monitoring and Healthcare Reporting

Provide dashboards showing control coverage, risk posture, and HISF compliance readiness.

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 Guidelines for Health Information Security

Provides implementation guidance to assist healthcare organizations in aligning with HISF 2022 requirements.

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

HISF 2022 Risk Assessment Procedures

Describes methodologies for conducting risk assessments under the HISF framework.

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

HISF 2022 Compliance and Auditing Framework

Outlines compliance requirements and auditing processes for healthcare providers.

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

Frequently asked questions

What is the New Zealand HISF 2022 used for?

The HISF 2022 is designed to help healthcare organizations identify, address, and manage cybersecurity risks to health information systems. Its controls safeguard sensitive patient data and support compliance with New Zealand health sector privacy and security regulations.

Is compliance with the HISF 2022 mandatory for healthcare organizations?

While HISF 2022 is not a formal certification, adherence is expected for organizations delivering healthcare services in New Zealand, especially those subject to regulatory oversight by Te Whatu Ora – Health New Zealand. Compliance is often mandated by government contracts, sector guidelines, or required for integration with other health providers.

What organizations fall within the scope of the HISF 2022?

The HISF 2022 applies to healthcare providers, government health agencies, and third-party IT service partners managing health data or supporting health information systems in New Zealand. The framework is relevant to any entity that stores, processes, or transmits sensitive patient information in the health sector.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What are the key concepts and required artifacts under HISF 2022?

Key requirements include documented risk assessments, comprehensive cybersecurity policies, incident response plans, and regular reviews of security controls. Organizations must establish privacy governance measures and maintain evidence demonstrating adherence to security practices.

How should organizations implement the HISF 2022?

Implementation involves integrating HISF requirements into organizational risk management processes, conducting regular threat and vulnerability assessments, and operationalizing technical and administrative controls. Ongoing education, incident response readiness, and continual improvement are also important.

How does the HISF 2022 relate to other cybersecurity frameworks or standards?

The HISF 2022 aligns with international best practices, such as ISO 27001 and NIST guidelines, but is tailored to the specific regulatory and operational context of the New Zealand healthcare sector. Organizations may map HISF controls to other frameworks to ensure comprehensive security coverage and compliance with multiple standards.

What are the ongoing compliance requirements for HISF 2022?

Healthcare organizations must conduct periodic risk assessments, monitor the effectiveness of implemented controls, update security policies, and maintain detailed compliance documentation. Incident response plans and continuous staff training are also required to address emerging threats and maintain resilience.

How would SmartSuite support New Zealand HISF 2022?

SmartSuite supports HISF 2022 compliance by enabling organizations to track cybersecurity risks, manage and document required security controls, collect evidence for audits, and generate compliance reports. Its platform helps maintain audit readiness, monitor security program maturity, and centralize policy and incident documentation to support ongoing regulatory adherence.

License included / downloadable: Yes The Health Information Security Framework (HISF 2022) is published by HISO under Te Whatu Ora and is freely available on the Te Whatu Ora website. License included with platform

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