hiso Health Information Standards Organisation
PAEREWA PĀRONGO HAUORA

Te Whatu Ora
Health New Zealand

Health Information Security Framework
Guidance for Micro to Small Organisations

HISO 10029.2:2023

Released April 2023

Te Kāwanatanga o Aotearoa
New Zealand Government

Citation: Te Whatu Ora – Health New Zealand. 2023. *HISO 10029.2:2023 Health Information Security Framework Guidance for Micro to Small Organisations*. Wellington: Te Whatu Ora – Health New Zealand.

Published in April 2023 by Te Whatu Ora – Health New Zealand
PO Box 793, Wellington 6140, New Zealand

ISBN 978-1-99-106715-9 (online)

Te Whatu Ora
Health New Zealand

This document is available at **tewhatuora.govt.nz**

Contents

Purpose

This document is published as part of the Health Information Security Framework (HISF) to provide cyber security guidance for micro to small organisations in the health sector. This segment is defined as health organisations that fall into two or more of the following categories:

- a stand-alone business/organisation
- based at a single geographic location with a basic technology setup (e.g., laptops, internet, relevant software)
- staffing of up to approximately 25 personnel
- manages a population of less than 10,000
- minimal or no IT support in-house (most IT services and support capability is outsourced to external IT and security vendors)
- is not involved with integrating or developing software systems or web applications in-house.

Implementation of the Health Information Security Framework within micro to small organisations is a three-step process:

- understanding the published core framework document HISO 10029:2022 Health Information Security Framework
- reading the guidance and understanding the requirements as outlined in this document for micro to small organisations
- using HISF Tools and Templates, as well as other approved materials to meet the requirements outlined within this guidance document.

Start by reading the core framework document which provides foundational information on the segments, building blocks, functional processes and principles of the framework, as well as the overall implementation approach. The requirements are linked to the relevant national and international standards as defined in the core framework document.

This guidance document for micro to small organisations contains the detailed level of control implementation for all requirements grouped under the identified functional processes. These are recommendations and it is important to note that there could be other ways of implementing controls to meet the requirement, in addition to those in the guidance section.

You are welcome to use HISF Tools and Templates (e.g., checklists, templates, and forms) that are provided to help support, assess, implement and document your control effectiveness against the documented requirements.

Cyber security requirements for micro to small organisations

The list below contains 21 cyber security requirements for micro to small organisations abbreviated as HMS (HISF Micro to Small). These requirements are grouped according to the five functional processes as defined in section **5 HISF Framework** from the core framework document.

PLAN	
HMS01	Information security roles and responsibilities are to be clearly defined.
HMS02	A defined health information security policy is documented and approved by management.
IDENTIFY	
HMS03	An inventory of assets where health information is stored, including software, endpoint devices and relevant owners are identified and maintained.
HMS04	All suppliers responsible for delivering health information related assets and services are to undergo periodic security assurance activities.
PROTECT	
HMS05	A security risk assessment is conducted periodically, and the identified risks are managed.
HMS06	Requirements are identified, and contractual obligations are met before the information is shared with authorised parties.
HMS07	Access to health information and endpoint devices is provided based on the legitimate business and health information security requirements and on the role of the individual.
HMS08	Latest operating systems, hardware devices, relevant software and internet browsers are used and kept up-to-date and where applicable, licensed versions are to be used.

HMS09	Permissions for all personnel is restricted so that external media, unauthorised or malicious software is not installed on devices that are used to store, process or transfer health information.
HMS10	Up-to-date anti-virus, anti-malware/endpoint security software is installed on all computers and servers to protect health information and endpoint devices against malicious code or software.
HMS11	All relevant health information is backed up securely (as outlined in your documented policy) in an encrypted format and restoration is tested periodically.
HMS12	Only authorised devices that are managed and have security controls in place are to be used to process health information.
HMS13	When personnel are working remotely, security measures are in place to protect health information which could be accessed, processed, or stored outside the organisation’s premises.
HMS14	Licensed and secure software, tools or services are used to manage health information.
HMS15	Network services used for transmitting and receiving health information and data are kept secure, to ensure minimal security impact upon clinical practice.
HMS16	Devices processing or storing or transmitting health information are connected, where possible, to a separate network with heightened security away from other information and assets.
HMS17	Web traffic is encrypted for public facing websites which contain health information, so that they are protected against Distributed Denial of Service (DDoS) attacks.

DETECT	
HMS18	All health information user activities are recorded, stored for a period of time and protected for analysis in case of a security incident.
HMS19	Unusual behaviour and potential information security incidents amongst endpoints and internal and external network traffic are detected.

RESPOND	
HMS20	A documented and approved security incident management process is maintained, reviewed, and tested periodically.
HMS21	Availability of health information is to be maintained in the event of a service, system, or application being disrupted for a prolonged period.

Requirements and guidance for micro to small organisations

Functional Process	Topic	Control	Requirement	Guidance
Plan	Governance	Information security roles and responsibilities	HMS01: Information security roles and responsibilities are to be clearly defined.	**Roles and Responsibilities** To protect health information, which is being stored or processed, the organisation is to define and manage the responsibilities required for information security risk management activities, including: • personnel are complying with policies (e.g., information security policy and acceptable use policy) • maintaining the risk register • managing and mitigating identified risks • providing security awareness education to personnel so that staff are aware of what to do and what not to do with health information • maintaining separation of duties so that there are no conflicting roles • performing periodic reviews to ensure the organisation and their suppliers are framework compliant. Individuals with allocated information security responsibilities, usually, a senior manager/director can assign security tasks to others. However, they ultimately remain accountable and are to check that any delegated tasks have been correctly performed.
Plan	Governance	Policies for information security	HMS02: A defined health information security policy is documented and approved by management.	**Information Security Policy** Creating an effective security policy addresses the implementation of security controls to mitigate or minimise potential threats. All organisations either processing, storing or transmitting health information are to develop and maintain an information security policy which contains a minimum of the sections below: • purpose of the policy document • scope of the policy i.e., is the scope limited to areas where health information is processed, used and managed or is extended to other areas of the organisation • legislative, regulatory, and contractual requirements, particularly those surrounding the protection of health information • notification of information security incidents, including a channel for raising concerns regarding confidentiality, without fear of blame or accusation for those reporting them

Functional Process	Topic	Control	Requirement	Guidance
				• the identification of processes and systems that are vital to healthcare, where failure of these processes could lead to adverse patient effects • outsourced services relating to patient care. Additionally, the policy is to be published, approved by management, communicated to all relevant personnel and reviewed at least yearly (or following a serious security incident or when risk assessments are performed). While creating the information security policy document, organisations will need to specifically consider the following factors, which are unique to the health sector: • the extent of health information covered by the policy • the responsibilities of staff, as agreed in the Acceptable Use Policy, and as accepted by members of professional bodies • the rights of patients, where applicable, to privacy and to access to their records • the obligations of clinicians with respect to obtaining informational consent from patients and maintaining the confidentiality of patient personally identifiable health information • the legitimate needs of clinicians and organisations to be able to overcome normal security protocols when healthcare priorities, often linked to the incapacity of certain patients to express their preferences, necessitate such overrides (including the procedures to achieve this) • the rules and procedures applied to the sharing of health information for the purposes of statistics, research and clinical trials • the system and location access arrangements for, and authority limits of, temporary staff (e.g., locums, students, “on-call” staff, volunteers, and support staff) • the impacts of security measures on patient safety • the impacts of information security measures on the performance of health information systems. The policy document is to be made available to all personnel electronically via intranet or shared drive and shared externally as per contractual obligations.
Identify	Asset Management	Inventory of information and assets	HMS03: An inventory of assets where health information is stored, including software and endpoint	**Asset Management Process** Managing assets benefits organisations in keeping them secure from malicious actors (from the point of procurement through to disposal). A documented and approved process, including the following is to be maintained by an organisation managing assets:

Functional Process	Topic	Control	Requirement	Guidance
			devices and relevant owners are identified and maintained.	• procurement of health devices from a known and authorised supplier or approved procedures (with relevant due diligence activities performed) • a designated custodian of health information assets • rules for acceptable use of assets are identified, documented, and implemented • secure sanitisation and destruction processes before disposal. **Asset Inventory** The inventory of assets (including software, hardware, servers, network devices, connected health network, laptops, desktops, mobile devices, telephony systems, cloud storage, etc) which are used to manage or process health information is to be accurate, up to date, consistent and aligned with other inventories. Options for ensuring accuracy of an inventory of information, software and endpoint devices include: • conducting periodic reviews of identified software and endpoint devices against the asset inventory • automatically enforcing an inventory update when installing, changing, or removing an asset. Documentation is to be maintained and updated as and when there are changes. The inventory of health information is to: • include rules for maintaining the financial value of health information assets and the integrity of these assets (e.g., the functional integrity of medical devices that record or report data) • the location where these assets reside. Medical devices that record or report data may require special security considerations depending on the environment they operate in (including potential electromagnetic emissions that may occur during their operation). Such devices are to be uniquely identified. Ensuring that inventories are maintained by their relevant functions, can create a set of dynamic inventories, including inventories for information assets, hardware, software, virtual machines (VMs), facilities, personnel, competence, capabilities, and records.

Functional Process	Topic	Control	Requirement	Guidance
				For identified health information, software and endpoint devices, ownership of maintenance is to be assigned to an individual or group. A process to ensure timely allocation of asset ownership should be implemented. Ownership is assigned when assets are created or transferred into the organisation. Asset ownership is reassigned as necessary when current asset owners leave or change roles. **Ownership of Assets** The organisation, when identifying health information assets, software and endpoint devices, are to determine their importance based on the level of information security and their owner. Documentation is to be maintained in dedicated or existing inventories. Assets include all health information that is captured, processed, transferred, stored, or recalled by the organisation and all devices and systems owned or used by the organisation for capturing, processing, transfer, storage or recall of health information. This includes all on and off premise devices, and service platforms used for these activities including specialist medical devices. While many information assets can be owned by the organisation in the conventional sense, it is important to note that the notion of ownership of health information is fraught with legal, ethical, and policy-based issues. Healthcare organisations and health professionals are often viewed as custodians or trustees in relation to personal health information. The asset owner is responsible for proper management of an asset over the whole asset life cycle, ensuring that: • health information and endpoint devices are inventoried • health information and endpoint devices are appropriately classified and protected • components supporting technology assets are listed and linked (i.e., database, storage, software components and sub-components) • requirements for the acceptable use of health information and endpoint devices are established • access restrictions are effective and reviewed periodically • health information and endpoint devices, when deleted or disposed, are handled in a secure manner, and removed from the inventory • they are involved in the identification and management of risks associated with the assets assigned • they support personnel who have roles and responsibilities in managing health information within the asset.

Functional Process	Topic	Control	Requirement	Guidance
Identify	Supplier Management	Supply Chain Risk Management	HMS04: All suppliers responsible for delivering health information related assets and services are to undergo periodic security assurance activities.	**Supply Chain Risk Management (SCRM)** SCRM is the process of identifying, assessing, and mitigating the risks of an organisation's supply chain. The risk of not managing your supply chain could lead to potential disruptions to the business or reputational damage, where there are failures by the supplier to meet their contractual obligations. Monitoring and reviewing of supplier services ensure: • the information security terms, and conditions of agreements are complied with, • any information security incidents and problems are managed properly, and • changes in supplier services or business status do not affect service delivery. **Contracts with Suppliers** To ensure sufficient support from the supplier for implementing security controls, investigations and recovery during an IT security incident, contracts are to include: • HISF compliance by the supplier • Security requirements per service i.e., Cloud service to go through a Cloud Risk Assessment (CRA), HISF to apply to telephony solution if conversations are recorded, etc as applicable • supplier responsibilities for incident response and subsequent level of support • supplier liability for loss in the event of a security incident, if found to be negligent. **Supplier Relationship** The responsibility for managing supplier relationships is to be assigned to a designated individual or team. Sufficient technical skills and resources are to be made available to monitor that the requirements of the agreement, in particular the information security requirements, are being met. Appropriate actions are to be taken when deficiencies in the service delivery are observed. **Supplier Relationship Management** A well-defined relationship between the organisation and the supplier are backed up with appropriate service level agreements. The implemented management controls ensure information security is enhanced over time, including: • reviewing service reports produced by the supplier and regular progress meetings (as required by the nature of the service and agreements) • monitoring service performance levels to verify compliance with the agreements

Functional Process	Topic	Control	Requirement	Guidance
				• periodic reviews to ensure suppliers are compliant with the framework. Alternatively, necessary controls are in place to manage any risks posed due to areas in which the organisation is deficient in • identifying any information security vulnerabilities and managing them • evaluating regularly that the suppliers are maintaining adequate information security controls • reviewing information security aspects of the supplier's relationships with their own suppliers • ensuring that the supplier continue sufficient service capability, and has workable plans designed to ensure agreed service continuity levels are maintained, following any major service failures or disasters • ensuring that suppliers assign responsibilities for reviewing compliance and enforcing the requirements of the agreements. Assurance activities of suppliers and sub-contractors are to be conducted prior to service acquisition and then periodically (every 12 months) for the duration of the supplier agreement. Assurance activities are to be carried out in conjunction with review of independent auditor reports such as ISO 27001, SOC 2 Type II, Cloud Security Alliance (CSA) reports etc. Issues identified are to be followed up with the relevant supplier and compensating controls implemented to manage the identified risks. **Management of Supplier Security Incidents** Security events that impact services provided by the supplier to the organisation are to be managed and reported on appropriately. Organisations are to: • respond to and manage any identified information security events or incidents • communicate effectively with the wider organisation that a security incident has occurred, and provide information in a timely manner • provide updates about information security incidents and review this information as required by the agreements (including any supporting guidelines and procedures) • review supplier audit trails and records of information security events, operational problems, failures, tracing of faults and disruptions related to the service delivered.

Functional Process	Topic	Control	Requirement	Guidance
				Managing Vulnerabilities Changes to the existing services or environment may be required to resolve known vulnerabilities. Monitoring these vulnerabilities are to include: • changes made by suppliers including: • enhancements to current services offered • development of any new applications and systems • modifications or updates to the supplier's policies and procedures • new or modified controls to resolve information security incidents and to improve information security • changes to supplier services including: • modifications and enhancements to networks • use of new technologies • adoption of new products or updated versions or releases • new development tools and environments • changes to physical location of service facilities • changes to supply chain • sub-contracting existing services to another supplier.
Protect	Risk Management	Information Security Risk Assessment	HMS05: A security risk assessment is conducted periodically, and the identified risks are managed.	**Risk Assessments** Risk assessments are performed to identify and manage hazards, reducing the likelihood of incidents occurring that could cause harm or put patient lives at risk. All organisations processing, storing, or transmitting health information are to perform risk assessments to identify: • controls which are effectively implemented • controls that need improvement • the additional controls the organisation needs to implement to reduce the health information security risk to an acceptable level. Risk assessment in healthcare frequently raises questions about information custodianship, ownership, and responsibility. Effective risk management ensures the alignment of responsibility for information security, with the authority to make risk management decisions. Risk assessments

Functional Process	Topic	Control	Requirement	Guidance
				are to be performed periodically (or when there is a significant change within the organisation) using a risk matrix which considers the impact of endpoint devices without restrictions. When documenting risks within the risk register, include the following: • document the risk including the potential cause and outcome (impact – patient, operational, financial, and contractual) • indicate risk status (open / closed / accepted) • identify the security controls or measures already in place • risk owner • date raised • determine the current threat likelihood, impact of the risk happening and overall risk level • identify existing controls to reduce, mitigate, transfer, or avoid the risk • identify security controls and acceptance criteria to either mitigate, avoid, transfer, or accept the risk • estimate the risk likelihood and impact of the risk occurring, and risk level • date of next review. While treating a risk to an acceptable state, the organisation is to ensure that spending on information security improvement is justified and represents a demonstrably good use of financial resources. This leads to the organisation defining and documenting their criteria for acceptance of risks, where health-specific factors (like below) need to be considered: • health sector, industry, or organisational standards • clinical priorities • impacts on patients. Identified risks related to patient safety need to be carefully analysed and explicitly addressed. These risk assessments are to be performed at a minimum of every year, or when: • a new service or application is introduced by the organisation that affects health information and associated devices • an existing service or application is being modified • there is a change in a supplier

Functional Process	Topic	Control	Requirement	Guidance
				- a serious security incident occurs. It is strongly recommended that the risk matrix the organisation is going to use is identified, and a risk register is maintained at an organisational level (including information security risks).
Protect	Information Sharing	Protection of health information	HMS06: Requirements are identified, and contractual obligations are met before the information is shared with authorised parties.	**Information Security Policy** All organisations storing, processing, and transmitting health information are to have an Information Security Policy (which contains rules for all relevant personnel to protect health information). The developed policies are to be made available to all relevant stakeholders involved in processing or storing or transmitting health information. Responsibility for handling health information is to consider all relevant legislation and regulations, contracts, and roles and responsibilities of the personnel handling the information and security controls. All personnel are to be made aware of their health information security responsibilities during onboarding processes. **Information Sharing Processes** Appropriate technical and organisational measures to support decision making for health professionals sharing health information are to be implemented. This also helps to protect health information by ensuring that any information shared is adequate and fit for purpose. Apart from contractual obligations, where possible, consent for sharing information is to be obtained from patients before their health information is e-mailed, faxed, communicated by telephone conversation, or otherwise disclosed to parties external to the healthcare organisation (e.g., insurance providers). **Contractual Agreements** Organisations are to include the approved methods of sharing health information securely between themselves and other organisations. This could be either via contractual or Master Service Agreements (MSAs) or part of collective agreements. A representative of each side of the agreement oversees the way health information is shared when there is a requirement. Processes are to be developed accordingly, to maintain the security of information while it is being shared.

Functional Process	Topic	Control	Requirement	Guidance
				Use of Encryption Encryption of information while being shared helps protect health data from unwanted users accessing sensitive information. Health information is to be encrypted before sharing via email, external hard drives, or USBs unless personal identifiable information is anonymised.
Protect	Access Management	Access Control and Secure Authentication	HMS07: Access to health information and endpoint devices is provided based on the legitimate business and health information security requirements and on the role of the individual.	**Access Creation and Revocation** Organisations storing, processing, or transmitting health information are to have a process(es) for assigning and/or removing both physical and logical access rights (including access to medical devices) for personnel. The process(es) is to include: • authorisation from the asset owner (or approval for access rights by other authorised personnel where appropriate). This is to be granted following any required background and relevant qualification checks • considering separation of duties (i.e., separating the roles of approval and implementation of access rights, or separation of other conflicting roles) • ensuring access is removed in a timely manner when someone no longer needs access to health information and endpoint devices (especially when personnel are leaving the organisation) • considering providing temporary access rights for a limited time period and removing them at the expiration date (in particular for temporary personnel such as locums, or where only temporary access is required by personnel) • verifying that the level of access granted is required, consistent with role responsibilities, and meets other information security requirements (such as separation of duties) • ensuring that access is activated (e.g., by service providers) only after all authorisation procedures are successfully completed • maintaining a central record of health information, software, and endpoint devices access rights granted to a user identifier (ID, logical or physical) • modifying access rights of users who have changed roles or jobs • maintaining a record of changes to users’ logical and physical access rights. **Access Reviews** Reviews of physical and logical access rights are to be performed periodically while considering the following:

Functional Process	Topic	Control	Requirement	Guidance
				• users' access rights after any role change within the same organisation, or following termination of employment • authorisations for elevated permissions to access the health information. **Employment Contracts** Consideration is to be given to including clauses in personnel's Individual Employment Agreements (IEAs), contracts and service contracts that specify disciplinary actions if unauthorised access is attempted. **Authentication Procedures** Authentication procedures are important for ensuring only authorised users have access to health information systems and respective facilities. Authentication procedures to access health information is to include: • passwords (based on industry best practices) • enforcing strong authentication (also known as multi-factor authentication) for individual accounts with heightened permissions. Using a combination of multi-factor authentication, such as what you know (a password), what you have (a token) and what you are (fingerprint or iris scan) reduces the possibilities for unauthorised accesses. Multi-factor authentication could also be combined with other controls to require additional factors under specific circumstances, based on predefined rules and patterns (such as access from an unusual location, from an unusual device or at an unusual time). The strength of authentication is to be appropriate for the classification of the health information being accessed. Where strong authentication and identity verification is required, authentication methods alternative to passwords, such as digital certificates, smart cards, tokens, or biometrics, are to be used. For pharmaceutical systems containing patient health information, biometrics or smart cards are usually preferred as authentication mechanisms for frequent and quick logons to the same device.

Functional Process	Topic	Control	Requirement	Guidance
				Legacy Systems Legacy systems i.e., older technology systems, may not allow multi-factor authentication to be implemented. If this occurs, these exceptions are to be added to an exception register, including a valid business need for using the system, along with approval from the authorised personnel to manage the risk.
Protect	Device Management	Management of Technical Vulnerabilities	HMS08: Latest operating systems, hardware devices, relevant software and internet browsers are used and kept up-to-date and where applicable, licensed versions are to be used.	**Automatic Updates** Where applicable, it is recommended to configure automatic updates to ensure the latest security patches are installed. Otherwise, latest versions, without known vulnerabilities are to be used. For acquired software, suppliers regularly release information about security updates for their software and provide a facility to install these automatically. Mechanisms are to be made available for the authorised personnel to decide whether to use the automatic update or not based on their business and security requirements. It is important that automatic updates which are enforced by the organisation are not turned off. Where the supplier or manufacturer provides an update process and updates can be installed on affected health systems without the need for intervention, the organisation determines if it applies the automated process or not. One reason for not using automated updates is to retain control over when the update is performed. i.e., if a piece of software is required for business operations, then it cannot be updated until the operation has completed, otherwise it would cause disruption. The organisation would then however have to register themselves to be notified of updates for the services, systems or devices which are being used in their facility. **Manual Updates** Organisations are to maintain a list of software (including which respective versions are being used) along with the hardware devices (i.e., laptops, desktops, telephone equipment, printers, server, tablets, internet connectivity devices) used to process, store, or manage health information (unless they are automatically updated). If any updates are to be performed by the supplier, a formal change management process is to be followed to capture the changes being made. It is strongly recommended uninstalling or disabling unsupported versions of software, as they no longer receive updates for security patches which leaves them vulnerable to attack.

Functional Process	Topic	Control	Requirement	Guidance
				Cloud Based Applications Where the organisation uses a cloud service, the technical vulnerability management of said cloud service is to be managed by the cloud service provider. The cloud service provider's responsibilities for technical vulnerability management are to be part of the cloud service agreement, including processes for reporting the cloud service provider's actions relating to any technical vulnerabilities. Organisations are responsible for vulnerability management of their own assets used for accessing the cloud services. **Hardware Refresh** Computing hardware such as laptops, desktops and servers are to be refreshed at least every 5 years to ensure enough computing power to run the operating system and applications. Additionally, it ensures hardware is still under manufacturer support, and that they are still issuing hardware patches for security vulnerabilities. **Legacy Systems** Legacy operating systems, hardware devices, software and internet browsers may be out of support by the supplier and patches no longer issued, in which case their continued use is to be added to the exceptions register, including a valid business use case and approval from authorised personnel to manage the risk. **Bring Your Own Device (BYOD) Requirements** For those using personal devices to store patient health information, a combination of automatic and manual updates is recommended to maintain the latest security patches for operating systems, internet browsers and hardware. Hardware refresh and legacy system procedures also apply to BYOD.
Protect	Device Management	Installation of software on operational systems	HMS09: Permissions for all personnel is restricted so that external media, unauthorised or malicious software is not installed on devices that are used to store, process or transfer health information.	**Restrict External Devices and Media** Users are to be restricted from using unauthorised external media on endpoint devices and are only allowed to use Bluetooth devices unless otherwise explicitly required (in which case storage media is to be configured to scan for malware upon plug in to the computer). This prevents the devices from being accidentally accessed by malicious users.

Functional Process	Topic	Control	Requirement	Guidance
				A list of approved software and approved devices (e.g., Bluetooth devices, encrypted USB sticks, etc) is to be made available to all relevant personnel accessing health information within the organisation (usually via the intranet or shared drive). **New or Software Enhancements** All new software requests or enhancements to existing permissions are to go through a documented and approved procurement process. Licensed versions, where applicable, are to be used. Software installation is to be performed by authorised personnel who have heightened permissions only. While performing software upgrades, to ensure the confidentiality and integrity of health information, a minimum of the following is to be considered: • business and security requirements assessed on a release-by-release basis • information security vulnerabilities are removed or reduced • operational software is updated only by trained administrators following appropriate management authorisation • only approved executable code (no development code or compilers) is installed on operational systems • testing is performed on a spare device off the network, before subsequently installing and updating software on all devices • maintaining documentation of all updates • a rollback strategy is defined before implementing any changes. Organisations are to consider the risks of relying on unsupported, unmaintained, and open-source software being used within the organisational environment.
Protect	Device Management	Protection against malware	HMS10: Up-to-date anti-virus, anti-malware/endpoint security software is installed on all computers and servers to protect health information and endpoint devices against malicious code or software.	**Anti-malware Software** Organisations that process, manage, or store health information are to implement appropriate prevention, detection, and response controls to protect against malicious software, including implementing appropriate user awareness training. Anti-virus, anti-malware / endpoint security software is to be installed on all endpoint devices (i.e., servers, laptops, desktops, mobile phones, including BYOD etc where applicable) and configured in such a way that they are auto updated.

Functional Process	Topic	Control	Requirement	Guidance
				Some medical devices may be an exception as not all manufacturers support additional installations from what is originally configured. If there is no mechanism to install additional software on medical devices, especially if they have internet connectivity, risks are to be identified before they are connected to the network and managed by implementing any available additional controls. Use of anti-malware software is effective if the below are considered: • scanning any data received over networks or via any form of electronic storage media (e.g., external hard drives, USBs), for malware before use • scanning email and instant messaging attachments and downloads for malware before use and carrying out this scan at different places (e.g., at email servers, desktop computers and when entering the network of the organisation) • scanning webpages for malware when accessed • protecting against the introduction of malware during maintenance and emergency procedures, which can bypass normal controls against malware • automatic update of virus signatures on all endpoint (servers, desktops, laptops, mobile phones) and medical devices (based on configuration from the manufacturer). **Exceptions** Some assets within the organisation cannot always be protected by anti-malware software (e.g., medical devices, mobile phones, access points) due to configuration restrictions, which should therefore be temporarily or permanently disabled during maintenance or emergency procedures. Such requirements follow a process for authorisation and approval from a senior manager/director where the review date, along with the business justification, are documented and maintained for reference purposes and further action. For medical devices, it is not always possible to install anti-malware software due to configuration restrictions. Risks of non-existence of anti-malware are to be identified in such cases and managed with alternate controls in place (e.g., devices which are internet connected are on a separate network). **Infected Devices** Some forms of malware infect computer operating systems and computer firmware to the extent that common malware controls cannot clean the system. In these instances, a full reimaging of the

Functional Process	Topic	Control	Requirement	Guidance
				operating system software and sometimes the computer firmware is necessary to return to a secure state. If any device is found to be infected with malware, it is to be reported to relevant personnel and incident management procedures are to be followed.
Protect	Device Management	Information backup	HMS11: All relevant health information is backed up securely (as outlined in your documented policy) in an encrypted format and restoration is tested periodically.	**Backups** Backups of health information, to create a copy which can be recovered in the event of data unavailability or failure should be performed at organisations processing or storing health information. The need to backup health information, based on a Critical Systems and Services Analysis (otherwise known as a Business Impact Analysis), is to be determined by the organisation. To address data retention, a backup procedure can be documented and approved as per business and security requirements. The documented procedure ensures that all essential health information and software can be recovered following an incident or failure or loss of storage media. When designing a backup plan, a minimum of the following is to be considered: • complete, successful, and secure backups are to be performed • the frequency of the backups meets the business and security requirements of the organisation • backups (e.g., tapes) are stored in a safe and secure remote location • giving backup information an appropriate level of physical and environmental protection, consistent with the standards applied at the main site • end to end encryption of cloud backups based on the criticality of the information (and in line with industry best practices). For example, protect the file with a password and share the password with the recipients via text or a separate email • restoration procedures are documented and tested at least quarterly on a test system, and not by overwriting the original storage media. Authorised personnel are to monitor the execution of backups and address failures of scheduled backups to ensure completeness. Where cloud services are being used, backup copies of the health information and application configuration in the cloud service environment are to be considered. It is important to note that information stored on mobile devices may not always be backed up (e.g., because of limited network bandwidth or because the devices are not connected at the times when backups are scheduled).

Functional Process	Topic	Control	Requirement	Guidance
				Restoration Restoration procedures ensure that they can be relied on for emergency use when necessary. These procedures are to be periodically tested to ensure the objectives of incident response and business continuity plans are met. In the case of critical health systems and services, backup measures are to cover all health systems information, applications, and data necessary to recover the complete system in the event of a disaster. **Retention Period** Retention period for the backed-up health information is to be determined, considering any requirement for retention of archive copies. If the retained health information is no longer required as per legal, regulatory, and contractual obligations, secure disposal procedures are to be considered.
Protect	Device Management	User endpoint devices	HMS12: Only authorised devices that are managed and have security controls in place are to be used to process health information.	**Secure Device Configuration** Organisations have documented and approved procedures for secure configuration of the devices being used to handle health information. This helps reduce unnecessary cybersecurity vulnerabilities. These procedures are to be communicated to relevant personnel and the following are to be considered for both managed devices and personal devices: • the type of information and the classification level that the user endpoint devices can handle, process, store, or support • requirements for physical protection of devices • restriction of software installation (e.g., remotely controlled by system administrators) • requirements for user endpoint device software (including software versions) and for applying updates (e.g., active automatic updating) • rules for connection to information services, public networks, or any other network off premises (e.g., requiring the use of personal firewall) • access controls • storage device encryption • protection against malware • remote disabling, deletion, or lockout • secure backups

Functional Process	Topic	Control	Requirement	Guidance
				• usage of web services and web applications • end user behaviour analytics • the use of removable devices, including removable memory devices, and the possibility of disabling physical ports (e.g., USB ports) • the use of partitioning capabilities, if supported by the user endpoint device, which can securely separate the organisation's information from personal information on the device. To protect the endpoint devices from data leaks and data loss, organisations are to consider the following: • configuring devices so that they are only connected to authorised networks (e.g., a specific network while working on-premises and connecting to a network with password while working remotely) • licensed versions of software are used • how health information is backed up if on remote devices. While personnel are accessing sensitive health information, measures are in place to restrict storage of local copies on devices. This could be achieved by disabling file downloads and reading information from local storage such as USBs. All personnel are to be made aware of the security requirements and procedures for protecting endpoint devices, including their responsibilities for implementing security measures. Personnel are advised to: • log-off active sessions and terminate services when no longer needed • protect user endpoint devices from unauthorised use with a physical control (e.g., key lock or special locks) and logical control (e.g., password access) when not in use • not leave devices carrying important, sensitive health information unattended • use devices with special care in public places, open offices, meeting places and other unprotected areas (e.g., avoid reading if people can shoulder surf, use privacy screen filters) • physically protect user endpoint devices against theft (e.g., don’t leave unattended in cars and other forms of transport, hotel rooms, conference centres and meeting places).

Functional Process	Topic	Control	Requirement	Guidance
				Personal Devices If an organisation allows the use of personal devices (sometimes known as BYOD), the following are to be considered: • separation of personal and business use of the devices (including using software to support such separation and protect business data on a private device) • providing access to health and business information only after users have acknowledged their duties (physical protection, software updating, etc.), waiving ownership of business data, and allowing remote wiping of health data by the organisation (in case of theft or loss of the device or when no longer authorised to use the services) • that health information is not to be photographed by insecure devices or sent by personal email. **Use of Encryption** Encryption of information while being shared helps protect health data from unwanted users accessing sensitive information. Health information is to be encrypted before sharing via emails, external hard drives, USBs unless personal identifiable information is anonymised. **Lost or Stolen Devices** If any devices are lost or stolen, incident management processes are to be followed taking legal, statutory, regulatory, contractual (including insurance) and other security requirements into consideration.
Protect	Device Management	Remote working	HMS13: When personnel are working remotely, security measures are in place to protect health information which could be accessed, processed, or stored outside the organisation’s premises.	**Remote Working** Organisations sometimes work remotely (i.e., not from the practice). IT support is needed for secure remote working tools. Where applicable, the following remote working tools and security practices are to be considered: • use of Virtual Private Networks (VPN) or Virtual Desktop Interface (VDI) for secure connectivity to the organisation’s environment • the existing or proposed physical security of the remote working site (e.g., lockable filing cabinets, clear desk, printing, and disposal of information) • rules and security mechanisms for the remote physical environment (such as endpoint devices), and information security event reporting

Functional Process	Topic	Control	Requirement	Guidance
				• the expected physical remote working environment and secure transportation between locations • communications security requirements, considering the need for remote access to the organisation’s systems, the sensitivity of the information to be accessed and shared over the communication link, and the sensitivity of the information contained in required systems and applications • the threat of unauthorised access to information or resources from other persons at the remote working site (e.g., family and friends) • the threat of unauthorised access to information or resources from other persons in public places • the use of home networks and public networks, and requirements or restrictions on the configuration of wireless network services • use of security measures, such as firewalls and protection against malware • secure mechanisms for deploying and initialising systems remotely • secure mechanisms for authentication and enablement of access privileges, taking into consideration the vulnerability of single-factor authentication mechanisms where remote access to the organisation’s network is allowed. Personnel who are working from remote locations are to abide by the guidelines on remote working which are issued by the organisation. The guidelines and measures to be considered are to include: • the provision of suitable equipment and storage furniture for remote working activities, where use of privately-owned equipment not under the control of the organisation is not allowed • a definition of the work permitted and the classification of information that can be held, including which internal systems and services the remote worker is authorised to access • the provision of training for those working remotely and those providing support. This is to include how to conduct business in a secure manner while working remotely • the provision of suitable communication equipment, including methods for securing remote access, such as requirements on device screen locks and inactivity timers; the enabling of device location tracking; installation of remote wipe capabilities • physical security • rules and guidance on family and visitor access to equipment and information

Functional Process	Topic	Control	Requirement	Guidance
				• the provision of hardware and software support and maintenance • the provision of insurance • the procedures for backup and business continuity • audit and security monitoring • revocation of authority and access rights and the return of equipment when the remote working activities are terminated.
Protect	Information Sharing	Data Leakage Prevention	HMS14: Licensed and secure software, tools or services are used to manage health information.	**Use of Licensed and Secure Systems** When acquiring new software, tools or services within the organisation, they are to be approved by management considering a minimum-security criteria. To help assess the viability of a desired software, a minimum of the following is to be considered: • there is ongoing maintenance and 24/7 customer support • capability of handling security incidents • security management and control features, including: • multi-factor authentication (MFA) • backups and restore functionality • ability to access software with registered accounts • the information shared or used within the software is encrypted • ability to remove information when the software is no longer being used, or as per business needs • activities that are being performed i.e., modification, deletion of information are being tracked and offer audit trails • measure the viability of the supplier by: • checking for recent security breaches • reviewing references from previous successful engagements within the industry and within the region • reviewing independent third-party assurance reports (such as SOC 2 Type II, ISO Certifications or Cloud Security Alliance (CSA) STAR Certification, etc) to ensure that the required scope of the acquired service(s) is being covered

Functional Process	Topic	Control	Requirement	Guidance
				The use of licensed software is always to be considered, as in all cases it is to include stronger contractual obligations and commitment on the supplier side to help assist with assurance, management, and security requirements. With any existing software, tools or services being used (e.g., Gmail and Hotmail) a review is recommended to be performed at least annually to ensure they remain current, fit for purpose and the above-mentioned pointers are considered.
Protect	Network Management	Security of networks	HMS15: Network services used for transmitting and receiving health information and data are kept secure, to ensure minimal security impact upon clinical practice.	**Network** A network is a combination of two or more computing devices that are interconnected by a wired or wireless communication for sharing of resources or information. **Network Services** Network services include the provision of connections, private network services and managed network security solutions such as firewalls and intrusion detection systems. These services can range from simple unmanaged bandwidth to complex value-added offerings. Network service arrangements such as HealthLink for pharmacies and Connected Health for GPs are in place. **Network Security Measures** The security measures necessary for services, such as security features, service levels and service requirements, are to be identified and implemented (by internal or external network service providers). Organisations processing or transmitting health information are to ensure that network service providers implement these measures. Rules on the use of networks and network services are to be implemented to cover: • the networks and network services which can be accessed • authentication requirements for accessing various network services • authorisation procedures for determining who is allowed to access which networks and networked services • network management and technological controls and procedures to protect access to network connections and network services • the means used to access networks and network services (e.g., use of virtual private network [VPN] or wireless network) • time, location, and other attributes of the user at the time of the access • monitoring of the use of network services.

Functional Process	Topic	Control	Requirement	Guidance
				The ability of the network service provider to manage agreed services in a secure way is to be assessed and regularly monitored. The organisation is also to consider third-party reviews provided by service providers to demonstrate they maintain appropriate security measures. **Network Security Features** The following network services' security features are to be considered: • technology used for security of network services, such as authentication, encryption, and network connection controls • technical parameters required for secured connection with the network services (in accordance with the security and network connection rules) • caching (e.g., in a content delivery network) and its parameters that allow users to choose the use of caching in accordance with performance, availability and confidentiality requirements • procedures for network service usage, to restrict access to network services or applications, where necessary.
Protect	Network Management	Separation of networks	HMS16: Devices processing or storing or transmitting health information are connected, where possible, to a separate network with heightened security away from other information and assets.	**Network Separation** The organisation considers managing the security of networks by dividing them into separate network domains or smaller networks (i.e., network segmentation) and separating them from the public network (i.e., internet). This helps in limiting the access to only those who need it. The separation can be done using either physically different networks or by using different logical networks. The assessment of network separation is to be in accordance with the access requirements, value and classification of information processed, taking into the relative cost and performance impacts of incorporating suitable gateway technology. Networks often extend beyond organisational boundaries, with business partnerships formed that require the interconnection or sharing of information processing and networking facilities. Such extensions can increase the risk of unauthorised access to the organisation's information systems that use the network, some of which require protection from other network users because of their sensitivity or criticality.

Functional Process	Topic	Control	Requirement	Guidance
				Networks Wireless networks require special treatment due to the poorly defined network perimeter. For sensitive environments, wireless access is to be separated from the internal network access, and guests given guest Wi-Fi access, which is separate to Wi-Fi access by personnel.
Protect	Operations Security	Encryption	HMS17: Web traffic is encrypted for public facing websites which contain health information, so that they are protected against Distributed Denial of Service (DDoS) attacks.	**Hosting Websites or Web Applications** Organisations using public facing websites to manage or process health information are to use encryption protocols as per industry best practice for external web traffic containing health information. This helps ensure that the confidentiality and integrity of information is maintained. Any website—static or dynamic—is to encrypt web traffic by having an SSL/TLS certificate for website encryption of the data it delivers to the web browser, with a safe HTTPS protocol so that website is secured, website credibility is increased and authentication to the website is provided. A static website provides the same sort of information that can be obtained from a brochure. A dynamic website allows you to create a user profile, comment on a post, book an appointment or purchase something. When booking patient appointments for example, it is important to secure patient information and web traffic. Organisations are to protect critical websites against DDoS attacks by: • implementing web application firewalls (WAFs) which can differentiate between DDoS attacks and legitimate traffic providing protection from potential cyber-attacks • hosting websites on a content delivery network (CDN) in the cloud, which makes it more difficult for hackers to find and attack the organisation’s webserver (since CDN uses a group of servers to deliver content online, it makes it harder for a hacker to identify the main server). Optimisations via a CDN also help lower the bandwidth that the primary server needs to use, making it less likely for the server to get overloaded • using a CDN’s secure port protocol to help prevent bad traffic from coming through.

Functional Process	Topic	Control	Requirement	Guidance
Detect	Operations Security	Logging	HMS18: All health information user activities are recorded, stored for a period of time and protected for analysis in case of a security incident.	**Logging** Logs are generated by an operating system or application for errors, warnings, and informational events. Effective audit and logging can help uncover misuse of health information and endpoint devices. The audit logs generated on health information systems are to be made available for analysis, where individuals are identified based on their activities performed on the health systems, and the records of patients have been accessed or modified. Organisation's processing, storing, or transmitting health information are to create a secure audit record each time an individual access, creates, updates, or archives the information on the endpoint devices. The collected audit logs are to indicate the following for each event: • identify the individual • action performed by the individual • time and date, using synchronised time sources to allow for correlation of logs between systems for analysis, alerting and investigation of an incident • health information and associated asset for investigation purposes. While logging, a minimum of the following events is to be considered: • successful and rejected access attempts • successful and rejected data and other resource access attempts • changes to configuration • use of privileged access • use of utility programs and applications • files accessed and the type of access, including deletion of patient files • activation and deactivation of anti-virus or malware software • creation, modification, or deletion of user IDs • malicious code executed by personnel who have permissions. This could also include suppliers • log files cannot be deleted or altered by any personnel. Logs are to be protected from being tampered with (edited or deleted or over written) and reviewed to maintain accountability for the personnel who have access to them. This could be achieved by recording the logs in an append-only and read-only file. Some audit logs can be required to be archived because of requirements on data retention or requirements to collect and retain evidence.

Functional Process	Topic	Control	Requirement	Guidance
				Log management responsibilities can be shared between the service customer and the service provider in cloud environments. Responsibilities vary depending on the type of cloud service being used. For medical devices, generated logs are to be extracted as per manufacturers' documented instructions and are to be investigated either in-house (based on expertise) or securely shared to the organisation who performs the investigation. **Log Analysis** Personnel who perform log analysis are to have the appropriate operational knowledge, and analysis is to be performed based on the documented and approve procedures. While performing log analysis, the following are to be considered: • the required attributes of each security-related event • exceptions identified through use of predetermined rules • known behaviour patterns and standard network traffic, compared to irregular activity and behaviour [user and entity behaviour analytics (UEBA)] • results of trend or pattern analysis (e.g., from using data analytics, big data techniques and specialised analysis tools) • available threat intelligence • examining usage reports from suppliers (e.g., invoices or service reports) for unusual activity within systems and networks (e.g., by reviewing patterns of activity) • including event logs of physical monitoring such as entrance and exit times to ensure more accurate detection and incident analysis • correlating logs to enable efficient and highly accurate analysis. Collected logs are to be anonymised when they are being sent to a supplier for assistance with debugging or troubleshooting errors. The anonymisation is to extend to information such as usernames, internet protocol (IP) addresses, hostnames, and organisation name. If the logs contain privacy information, they are to be encrypted and sent securely to the vendor. Suspected and actual information security incidents are to be identified (e.g., malware infection or probing of firewalls) and subject to further investigation (e.g., as part of an information security

Functional Process	Topic	Control	Requirement	Guidance
				incident management process). For log monitoring, tools can be used to configure and optimise the benefits of effective analysis.
Detect	Operations Security	Real time monitoring	HMS19: Unusual behaviour and potential information security incidents amongst endpoints and internal and external network traffic are detected.	**Real Time Monitoring** Real time monitoring uses log information and intelligence on threats to increase the likelihood of identifying malicious activity early. While monitoring is being performed, a minimum of the following is to be considered: • outbound and inbound network, system, and application traffic • access to health information and endpoint devices including computing systems, servers, networking equipment, monitoring system, critical applications, etc. • critical or admin level system and network configuration files • logs from other tools (e.g., antivirus, endpoint detection and response [EDR], intrusion and detection system [IDS], intrusion prevention system [IPS], web filters, firewalls, data leakage prevention) • event logs relating to system and network activity • use of the computing resources (e.g., CPU, hard disks, memory, bandwidth) and their performance. The organisation is to establish a baseline where a minimum of the following is considered: • user behaviour for unusual activities • reviewing utilisation of systems and services during business and non-business hours • usual time of access, location of access, frequency of access for each user or group of users • unplanned pause or termination of systems or services • activity typically associated with malware or traffic originating from known malicious IP addresses or network domains (e.g., those associated with botnet command and control servers) • known attack characteristics (e.g., denial of service and buffer overflows) • unusual system behaviour (e.g., keystroke logging, process injection and deviations in use of standard protocols) • bottlenecks and overloads (e.g., network queuing, latency levels and network jitter)

Functional Process	Topic	Control	Requirement	Guidance
				• unauthorised access (actual or attempted) to systems or services containing health information • unauthorised scanning of applications, systems and networks • successful and unsuccessful attempts to access protected resources (e.g., DNS servers, web portals and file systems). **Automated Alerts on Thresholds** Automated monitoring software is to be configured to generate alerts based on predefined thresholds. The alerting system is to be tuned as required by the organisation's baseline, and personnel dedicated to respond to alerts are to be properly trained to detect potential incidents.
Respond	Incident Management	Information security incident management planning and preparation	HMS20: A documented, and approved security incident management process is maintained, reviewed and tested periodically.	**Information Security Incident Management** The objectives for health information security incident management are to be agreed with management. Those responsible for incident management must understand the organisation's priorities for handling health information security incidents, including an agreed resolution time frame, based on potential consequences and severity. Health incident management procedures are to be implemented to meet these objectives and priorities that are required for organisations processing, storing, or transmitting health information. **Security Event Reporting** All individuals are to be made aware of their responsibility to report information security events as quickly as possible to prevent or minimise the effect of information security incident. They are to be aware of the procedures for reporting information security events including incidents, breaches, vulnerabilities and the point of contact for which the events are to be reported to. The reporting mechanism is to be as easy, accessible, and available as possible. Situations to be considered for information security event reporting include: • stolen credentials • access violations • stolen or lost devices • suspected malware infection • financial fraud and unauthorised claims for patient treatment • ransomware • Distributed Denial of Service (DDoS) attacks.

Functional Process	Topic	Control	Requirement	Guidance
				Individuals are to be advised not to attempt to prove suspected information security vulnerabilities. As part of contractual agreements with the organisation’s suppliers, it is strongly recommended to include their required level of support for managing incidents as and when they arise. This could include having a RACI (Responsible, Accountable, Consulted, Informed) matrix readily available to know the parts of incident which are to be performed by suppliers, along with escalation contact points. **Security Incident Management Plan** Management is to ensure that a health information security incident management plan is created while considering different scenarios, with procedures developed and implemented for the following activities: • evaluation of security events pertaining to health information, and what criteria constitutes an information security incident • monitoring, detecting, classifying, analysing, and reporting security incidents • managing information security incidents to conclusion, including response and escalation, according to the type and the category of the incident (including possible activation of business continuity plans, controlled recovery from an incident and communication to internal and external interested parties) • coordination with internal and external interested parties such as authorities, external interest groups and forums, suppliers, and clients • logging incident management activities • handling of evidence • root cause analysis or post-mortem procedures • identification of lessons learned and any required improvements to the incident management procedures or information security controls These plans are to be tested periodically (not necessarily in production environments), reviewed, and stored for reference purposes.

Functional Process	Topic	Control	Requirement	Guidance
				Security Incident Roles and Responsibilities Roles and responsibilities for carrying out incident management procedures related to health information are to be determined and effectively communicated to the relevant internal and external interested parties. At a minimum, the following responsibilities are to be considered: • establishing a common method for reporting information security events, including point of contact (i.e., service desk or tool or email ID) • establishing an incident management process to manage health information security incidents, including administration, documentation, detection, triage, prioritisation, analysis, communication and coordinating interested parties • establishing an incident response process to provide the capability for assessing, responding to, and learning from health information security incidents • only allowing competent personnel to handle the issues related to information security incidents within the organisation. Such personnel are to be provided with incident handling procedure documentation and periodic training • communication to both internal and external parties is to be shared via authorised channels only. **Security Incident Response** In case of an event, the organisation is to establish and communicate procedures on health information security incident response to all relevant interested parties. Health information security incidents are to be responded to by a designated team with the required competency. The response is to include a minimum of: • containment, if the consequences of the incident can spread, so will the systems that are affected by the incident • collecting evidence as soon as possible after the occurrence • escalation, as required including crisis management activities and possibly invoking business continuity plans (BCPs) • ensuring that all involved response activities are properly logged for later analysis • communicating the existence of the health information security incident or any relevant details thereof to all relevant internal and external interested parties following the need-to-know principle

Functional Process	Topic	Control	Requirement	Guidance
				• coordinating with internal and external parties (such as authorities, external interest groups and forums, suppliers, and clients) to improve response effectiveness and help minimise consequences for other organisations • once the incident has been successfully addressed, formally closing and recording it • conducting information security forensic analysis (as required) • performing post-incident analysis to identify root cause. Ensure it is documented and communicated according to defined procedures • any external requirements on reporting of incidents to relevant interested parties within the defined timeframe (e.g., breach notification requirements to Te Whatu Ora, CertNZ) are to be considered • identifying and managing information security vulnerabilities and weaknesses, including those related to controls which have caused, contributed to, or failed to prevent the incident. Once the incident is contained or resolved, a post incident report (PIR) is recommended to provide a summary of the incident along with lessons learnt. If there are any existing processes or policies which need to be updated, the necessary documentation is to be updated, reviewed, approved, and communicated to all relevant parties. The reporting procedures are to include: • actions to be taken in case of an information security event (e.g., noting all pertinent details immediately such as malfunction occurring and messages on the screen, immediately reporting to the point of contact and only taking coordinated actions) • use of incident forms to support personnel to perform all necessary actions when reporting information security incidents • suitable feedback processes to ensure that those persons reporting information security events are notified, to the extent possible, of outcomes after the issue has been addressed and closed • creation of incident reports. **Infected Devices** Some forms of malware infect computer operating systems and computer firmware where common malware controls cannot clean the system, and a full reimaging of the operating system software (and sometimes the computer firmware) is necessary to return to a secure state. If any device is found to be infected with malware, it is to be reported to relevant personnel and incident management procedures are to be followed.

Functional Process	Topic	Control	Requirement	Guidance
				Lost or Stolen Devices If any devices are lost or stolen, incident management process is to be followed taking legal, statutory, regulatory, contractual (including insurance) and other security requirements into consideration.
Respond	Business Continuity Management	ICT readiness for business continuity	HMS 21: Availability of health information is to be maintained in the event of a service, system, or application being disrupted for a prolonged period.	**Business and ICT Services Continuity** In the context of continuous patient care, business continuity and ICT services continuity planning, it can be necessary to adapt the information security requirements from normal operational conditions depending on the type of disruption. The organisation is to determine their requirements for business continuity management processes and have established procedures for adapting information security controls during disruption. These processes are to be developed, tested, reviewed, and implemented (if necessary) to maintain or restore the security of critical health information following interruption or failure. Timelines for restoration of health information in case of disruption or failure are to be determined (i.e., a Critical Systems and Services analysis is to be performed to determine the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for the identified critical services and systems). While performing the analysis, the consequences for loss of confidentiality and integrity of health information are to be prioritised along with maintaining the need for availability. The analysis is usually performed along with the risk assessment process and risk management procedures.

Appendix A - Glossary

Term	Definition
Acceptable Use Policy	An agreement between two or more parties that outlines the appropriate use of access to a health service organisational network or the internet.
Authentication	Process for establishing an authenticator is genuine or as represented.
Authenticator	The means to confirm the identity of a user, process, or device (e.g., user password or token).
Authorisation	The rights or permissions granted to a system user to access a system resource.
Botnet	A collection of computers linked together to perform a specific task. They can be misused for malicious purposes to control a health service organisation's computer and use it to carry out attacks on devices outside the network.
Business Continuity Plan (BCP)	Documented procedures that guide organisations to respond, recover, resume, and restore to a pre-defined level of operation following disruption.
Bring Your Own Device (BYOD)	The practice of allowing employees of an organisation to use their own computers, smartphones, or other devices for work purposes.
Cloud Risk Assessment (CRA)	A tool used by organisations to help them identify and assess the risks arising from the use and handling of PHI and PII in the cloud. A CRA will also propose ways to mitigate or minimise these risks.
Content Delivery Network (CDN)	This uses a group of servers from different geographic locations to deliver web content online, to ensure that content is available at all times. This makes it hard for an attacker to identify and disrupt the main server.

Term	Definition
Critical Systems and Services Analysis	A process and corresponding toolset for identifying those cyber assets that are most critical to the accomplishment of an organisation's mission.
Denial of Service (DOS)	The prevention of authorised access to systems or the delaying of time-critical operations.
Distributed Denial of Service (DDOS)	A denial-of-service technique that uses numerous hosts to perform the attack to prevent authorised access to systems or the delay of time-critical operations.
Domain Name Server (DNS)	A server that translates requests for human readable names like www.example.com into the numeric IP addresses like 192.0.2.1, controlling which server an end user will reach when they type a domain name into their web browser.
Encryption	The process of a confidentiality mode that transforms usable data into an unreadable form (ciphertext) using a cryptographic algorithm and key.
Endpoint detection and response (EDR)	A solution that continuously monitors end-user devices to detect and respond to cyber threats like ransomware and malware.
Health information	This includes personal health information (PHI), patient identifiable information (PII).
Health information assets	This includes paper based and digitally stored health information, computing devices (e.g., computers, servers, mobile phones), printers, network equipment, specialist medical devices, media storage, that contain health information or support the implementation of general IT controls for a health service organisation.
Incident	A breach of the security rules for a system or service, such as: • attempts to gain unauthorised access to a system and/or data

Term	Definition
	• unauthorised use of systems for the processing or storing of data • changes to a systems firmware, software, or hardware without the system owners' consent • malicious disruption and/or denial of service
Intrusion Detection System (IDS)	A monitoring software that looks for suspicious activity and alerts administrators.
Intrusion Prevention System (IPS)	System which can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its target.
Incident Response Plan	The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber-attacks against an organisation's information systems.
Latency	The time it takes for data to pass from one point of the network to another. For example, this could affect how quickly a webpage or application will load for users.
Legacy Systems	Operating systems, applications, internet browsers, computing and network hardware that are out of support by the supplier or manufacturer.
Malware	Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose.
Mitigate	A risk management strategy used to minimise the damage or impact of a threat until a problem can be remedied.
Multi-factor authentication	Using a combination of multiple authentication factors, such as what you know, what you have and what you are, reduces the possibilities for unauthorised accesses. Multi-factor authentication can be combined with other techniques to require additional factors under specific circumstances, based on predefined rules and patterns, such as access from an unusual location, from an unusual device or at an unusual time.

Term	Definition
Network segmentation	The security of large networks can be managed by dividing them into separate network domains or smaller networks and separating them from the public network (i.e., internet). This helps in limiting the access to only those who need it. The network domains can be separated based on levels of trust, criticality, and sensitivity (e.g., public access domain, desktop domain, server domain, low-risk, and high-risk systems), along with organisational units (e.g., human resources, finance, marketing) or some combination (e.g., server domain connecting to multiple organisational units). The separation can be done using either physically different networks or by using different logical networks.
Personal Health Information (PHI)	Demographic information, medical histories, test and laboratory results, mental health conditions, insurance information and other data that a healthcare professional collects to identify an individual directly or indirectly and determine appropriate care.
Patient Identifiable Information (PII)	Information pertaining to any person which makes it possible to identify such individual. This includes personal characteristics (e.g., height, weight, gender, date of birth, age, ethnicity, place of birth, biometrics information (such as fingerprints, DNA, retinal scans) and a unique set of numbers or characters assigned to a specific individual (e.g., name, address, telephone number, NHI number, email address, driver's license number, credit card number and associated PIN number, booking number).
Personnel	Organisational staff including permanent employees, fixed term employees and temporary roles, contractors, consultants, volunteers, locums, and staff from suppliers who processes or manages health information.
Post incident report (PIR)	Provides a summary of an incident along with the lessons learnt.

Term	Definition
RACI matrix	A Responsible, Accountable, Consulted, Informed (RACI) matrix is a tool that can support clarity on job roles and responsibilities. It is used to map out and document the key activities and deliverables for a function and the individuals or groups that have responsibility for their completion, signoff, and awareness.
Recovery Point Objective (RPO)	Maximum amount of data the organisation can tolerate losing.
Recovery Time Objective (RTO)	The maximum length of time it should take to restore normal operations following an outage or data loss.
Remediation	Implementing corrective action to eliminate a risk.
Residual risk rating	The measurement of risk (impact x likelihood) with suitable controls in place.
Risk	Security problems that an organisation could potentially face.
Risk Assessment	The process of identifying risks to a health provider organisation’s operations, assets, or individuals by determining the probability of occurrence, the resulting impact and additional security controls that would mitigate
Risk Register	A central record of current risks and related information for a health provider organisation. Current risks comprise of both accepted risks and risks that have planned mitigation activities in place.
Sanitisation	Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs.
Supply Chain Risk Management (SCRM)	The process of identifying, assessing, and mitigating the risks of the organisation’s supply chain.
Security control	A safeguard or countermeasure to avoid, detect, counteract, or minimize security risks to physical

Term	Definition
	property, information, computer devices, or other assets. Such controls protect the confidentiality, integrity, and availability of information.
Security Information and Event Management (SIEM)	A solution that helps organisations detect, analyse, and respond to security threats before they harm business operations. SIEM combines both security information management (SIM) and security event management (SEM) into one security management system. SIEM technology collects event log data from a range of sources, identifies activity that deviates from the norm with real-time analysis, and takes appropriate action. In short, SIEM gives organisations visibility into activity within their network so they can respond swiftly to potential cyberattacks and meet compliance requirements. In the past decade, SIEM technology has evolved to make threat detection and incident response smarter and faster with artificial intelligence.
Software firewall	A software-based firewall installed on a desktop or laptop computer to provide protection against external cyber attackers by shielding the computer from malicious or unnecessary network traffic. A software firewall can also prevent malicious software from accessing a computer via the internet.
Supplier	Service provider of on-premises or cloud services. e.g., Internet Service Provider, Outsourced Service Provider, Software as a Service (SaaS) provider.
Threat	Any event with the potential to adversely impact organisational operations, organisational assets, individuals, other organisations, through an information system via unauthorised access, destruction, disclosure, modification of information, and/or denial of service.

Term	Definition
Threat intelligence	Threat information that has been aggregated, transformed, analysed, interpreted, or enriched to provide the necessary context for decision-making processes.
User and entity behaviour analytics (UEBA)	A type of cyber security process that takes note of the normal user behaviour. In turn, they detect any anomalous behaviour or instances when there are deviations from these “normal” patterns. For example, if a particular user regularly downloads 10MB of files every day but suddenly downloads gigabytes of files, the system would be able to detect this anomaly and alert the administrator or manager immediately.
Virtual Machines (VMs)	It is no different to any other physical computer like a laptop, smart phone, or server. It has a CPU, memory, disks to store organisation files and can connect to the internet if needed. A VM is a computer file or an image that behaves like an actual computer. It can run in a window as a separate computing environment. The VM is partitioned from the rest of the system, meaning that software inside a VM can’t interfere with the host computer’s primary operating system.
Vulnerability	A weakness, or flaw, in software, a system or process. An attacker may seek to exploit a vulnerability to gain unauthorised access to a system.
Vulnerability Assessment	A systematic review of security weaknesses in an information system. It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities and recommends remediation or mitigation, if and whenever needed.
Vulnerability management	The ongoing, regular process of identifying, assessing, reporting on, managing and remediating cyber vulnerabilities across endpoints, workloads, and systems. Typically, a security specialist would leverage a vulnerability management tool to detect vulnerabilities and utilise different processes to patch or remediate them.

Term	Definition
Web application firewall (WAF)	Can protect web applications against common web exploits, cyber-attacks, and bots that can compromise the security and affect the availability of health information and associated services.