Security checklist

for health service providers

June 2026 – version 1.1

GENERAL PRACTICE NZ
The Heart of Health Care Networks

Health New Zealand
Te Whatu Ora

Cover note

This security checklist has been developed in collaboration with General Practice New Zealand (GPNZ) to support information sharing with Health New Zealand (Health NZ), such as for the Shared Digital Health Record and National Primary Care Dataset. It forms part of the assurance and due diligence obligations Health NZ has under the Government Digital Delivery Agency (GDDA) Information Sharing Standard and would be completed prior to signing the Access and Use Agreement and related service schedules for health services providers.

The checklist questions are based on the National Cyber Security Centre (NCSC) Minimum Cyber Security Standards. The ratings in this checklist are aligned to the Cyber Security Capability Maturity Model (CS-CMM) levels:

- Insufficient follows CS-CMM Level 1
- Baseline follows CS-CMM Level 2
- Better follows CS-CMM Level 3
- Best follows CS-CMM Level 4

Organisations delivering healthcare services who wish to access and share information with Health NZ, must comply with Cyber Security Capability Maturity Model Level 2 (CS-CMM 2), which is the 'Baseline' rating in this checklist[1]. It is expected that under the Shared Digital Health Record and National Primary Care Dataset agreements some health service provider organisations, such as those managing large information systems, are expected to meet either 'Better' or 'Best'.

This document has been designed to provide a breakdown of the CS-CMM requirements that are easy for organisations to understand and assess their cyber security maturity.

In addition to completing this maturity assessment, organisations are recommended to refer to HISO 10029 Health Information Security Framework (HISF) for guidance on the implementation of appropriate security controls for the nature and size of their organisation. HISF is recognised in the international Secure Controls Framework.

[1] This expectation was signalled by the Ministry of Health and Health New Zealand in a letter to the health sector dated 2 March 2026

Security checklist for health service providers

This checklist has been developed to support health service providers to confirm their cyber security arrangements meet the requirements for information sharing with Health NZ.

The checklist enables organisations to assess their current cyber security capability in a practical and consistent way, identify any gaps, and understand what is required to meet the **Baseline** level for participation in information sharing with Health New Zealand (Health NZ). The answers in the checklist are relied on by Health NZ in deciding whether an organisation is certified to connect to a Health NZ digital asset.

This checklist should be completed by a person with good knowledge of how your organisation works, who should consult with your IT providers and Primary Health Organisation (PHO) as necessary.

For each section:

- Read the descriptions from top to bottom
- Discuss what is currently in place at your organisation
- Tick the row that best describes where your organisation is today

Some of the controls described may be delivered by your IT provider, PHO, or other supporting services. What matters is that your organisation understands what security measures and arrangements are in place and who is responsible for delivering them, as a part of participating in information sharing with Health NZ. If you are unsure how to answer a question, you can ask your IT provider for clarification or contact your PHO for guidance and support.

Organisations are expected to meet at least the **Baseline** level across this checklist to proceed with information sharing.

The **Baseline** level represents a reasonable and achievable level of cyber security for most primary care practices and is aligned to the National Cyber Security Centre Minimum Cyber Security Standards. It focuses on having basic protections in place, clear responsibilities, and simple, documented processes.

Some organisations may already meet higher levels in certain areas, while others may identify actions needed to reach **Baseline** before proceeding.

Security checklist

Standard 1: Risk Management The organisation actively identifies, assesses, and manages cyber security risks as part of its day-to-day operations.			
Process requirement	**Description**	**Rating**	
1.1 Cyber security governance	A named person or group is responsible for cyber security in the organisation	**Insufficient:** No clear owner. Cyber security is assumed to be "IT's job".	☐
		Baseline: A director, practice manager, clinician, or management group is nominated and documented as responsible for cyber security. For example, one named person is documented as responsible for cyber security.	☐
		Better: Cyber security responsibility is embedded in governance and management structures; clear reporting lines to owners/board.	☐
		Best: Governance effectiveness is measured, e.g., frequency of reviews, completion of actions; adjustments made based on results.	☐

Standard 1: Risk Management

The organisation actively identifies, assesses, and manages cyber security risks as part of its day-to-day operations.

Process requirement	Description	Rating	
1.2 Cyber risk assessment	Cyber risks (ransomware, privacy breach, systems outage, supply chain) are identified and discussed alongside clinical and financial risks	**Insufficient:** Cyber risk is not formally considered or discussed.	☐
		Baseline: Cyber risk is assessed and discussed at least annually; documented in a risk register with controls identified, or in meeting minutes. For example, once a year, cyber risks (like ransomware or patient data being accessed incorrectly) are talked about at a leadership meeting and noted in meeting notes. This may be a simple list of cyber security risks alongside clinical and financial risks. Includes risks associated with the organisations information system providers and broader supply chain (e.g. third-party vendors, service providers, and software dependencies).	☐
		Better: Cyber risk assessment is integrated into routine governance (e.g., quarterly reviews); risks are prioritised and monitored.	☐
		Best: Risk metrics are tracked (e.g., number of incidents, time to remediate); risk appetite and tolerances are defined and reviewed in-line with board meetings.	☐

Standard 1: Risk Management

The organisation actively identifies, assesses, and manages cyber security risks as part of its day-to-day operations.

Process requirement	Description	Rating	
1.3 Critical systems register	An up-to-date list of business critical and externally facing systems (PMS, hosted servers, patient portal, e-prescribing, phones, lab and imaging access) is held securely, is maintained and updated on a regular basis	**Insufficient:** No current list. Knowledge is held informally by individuals.	☐
		Baseline: A documented list exists covering key business systems. For example, the organisation keeps a simple list (spreadsheet or document) of key systems such as the PMS, patient portal, email, e-prescribing, phone systems, lab/imaging access, so this information is available quickly during an outage or incident.	☐
		Better: The register is maintained as a living document; ownership, hosting, and security responsibilities are clear for each system.	☐
		Best: System criticality is assessed using defined criteria (e.g., patient safety impact, recovery time objective); register is reviewed and updated at least annually.	☐

Standard 1: Risk Management

The organisation actively identifies, assesses, and manages cyber security risks as part of its day-to-day operations.

Process requirement	Description	Rating	
1.4 Change management	Significant IT changes (new cloud systems or integrations) include a cyber security check before approval	**Insufficient:** Changes happen ad-hoc without security consideration. For example, there are no checks prior to the implementation of changes, or the organisation relies on their software vendor to make all changes and does not approve these prior to implementation.	☐
		Baseline: New systems and changes are subject to a basic security/risk check before approval and documented in a change request or approval record. For example, before a new system is added or a major IT change is made, someone at the organisation checks whether it could affect patient data or security and records that this check was done.	☐
		Better: Security checks are standardised using a checklist or template and is embedded in the organisation's change approval process.	☐
		Best: Change related security incidents are tracked; lessons learned are used to refine the security assessment process.	☐

Standard 2: Security Awareness

The organisation ensures that all staff understand their role in protecting patient information and organisation systems from cyber threats.

Process requirement	Description	Rating	
2.1 Induction training	All staff receive basic cyber security training at induction (phishing, passwords, handling patient information)	**Insufficient:** There is no training.	☐
		Baseline: All new staff receive documented cyber security training as part of induction. For example, new staff are shown basic guidance during induction on safe passwords, phishing emails, and how to handle patient information. This is written down or included in induction materials.	☐
		Better: Induction training uses standardised materials and is recorded; completion is tracked, e.g. the organisation uses a formal security training induction.	☐
		Best: Training completion rates and knowledge retention (e.g., via post-training quiz or phishing simulation results) are measured and reported.	☐

Standard 2: Security Awareness

The organisation ensures that all staff understand their role in protecting patient information and organisation systems from cyber threats.

Process requirement	Description	Rating	
2.2 Ongoing awareness	Staff receive refresher cyber security training or awareness at least annually	**Insufficient:** No ongoing training; staff rely on initial induction only, e.g. training only given once and not repeated.	☐
		Baseline: Annual refresher training or awareness sessions are scheduled and delivered. For example, once a year, staff receive a short refresher (such as an organisation education session, online module, or team meeting update) reminding them how to stay safe online and report issues.	☐
		Better: Ongoing awareness is embedded (e.g., regular tips, simulated phishing, scenario discussions); tailored to roles.	☐
		Best: Awareness programme effectiveness is measured (e.g., phishing click rates, incident reporting rates); programme adjusted based on data.	☐

Standard 2: Security Awareness

The organisation ensures that all staff understand their role in protecting patient information and organisation systems from cyber threats.

Process requirement	Description	Rating	
2.3 Incident reporting culture	Suspicious emails and potential incidents are reported (not just deleted) so IT can investigate and block similar attacks	**Insufficient:** Staff delete suspicious emails; incidents are rarely reported.	☐
		Baseline: Staff know how to report suspicious activity; basic reporting process is documented and communicated. For example, staff know exactly how to report suspicious emails or incidents (such as who to email or call) and this process is written down and shared with everyone.	☐
		Better: Reporting is easy and normalised; feedback loop exists (staff are told outcome and what to look for next time).	☐
		Best: Reporting metrics are tracked (e.g., number of reports, time to response, false positive rate); used to refine detection and training.	☐

Standard 2: Security Awareness

The organisation ensures that all staff understand their role in protecting patient information and organisation systems from cyber threats.

Process requirement	Description	Rating	
2.4 Secure communication	Staff avoid using plain email for sensitive patient information, or use secure methods	**Insufficient:** Sensitive information is routinely sent via plain email without controls.	☐
		Baseline: Staff are aware of risks and avoid sensitive information in unencrypted email where possible. Alternative communication mechanisms are in place (e.g., secure portal, encrypted email, text prompt, or phone calls for sensitive matters). For example, staff know about different ways to send communications with sensitive patient information and the risks of each. If email is the only practical option, they understand the risks and double-check the recipient list before sending.	☐
		Better: Secure communication is standard practice; monitored through periodic audits or spot checks.	☐
		Best: Compliance is measured (e.g., audit findings, privacy near-miss reports); corrective actions are tracked and reviewed.	☐

Standard 3: Asset Importance

The organisation identifies and prioritises assets that support critical functions using a risk-based approach.

Process requirement	Description	Rating	
3.1 Secure systems	All computers and servers that handle patient information are supported and receive security patches	**Insufficient:** Some devices are unsupported or end-of-life; patching (e.g., software updates to fix issues or vulnerabilities) is inconsistent.	☐
		Baseline: All devices handling patient data are supported; patch schedules are documented in IT support agreements. For example, computers with access to patient information have system updates installed regularly (by the organisation or an IT provider) and don't use end-of-life operating systems or software, like Windows 10 or internet browsers.	☐
		Better: Asset lifecycle management is embedded; end-of-life equipment and software is replaced proactively before support ends.	☐
		Best: Asset age, support status and patch compliance are tracked; reported to governance and used to plan replacements.	☐

Standard 3: Asset Importance

The organisation identifies and prioritises assets that support critical functions using a risk-based approach.

Process requirement	Description	Rating	
3.2 Data location and hosting	The organisation knows which systems hold patient data and where they are located (on-premises vs hosted/cloud)	**Insufficient:** Data locations are unclear; knowledge is held informally.	☐
		Baseline: Data locations are documented for all key systems; hosting responsibilities are clear (health service provider organisation, IT provider, or cloud vendor). For example, the organisation or IT provider knows which systems store patient data, whether they are on a server in the practice or hosted online, and who is responsible for managing each one.	☐
		Better: Data inventory is maintained and reviewed at least annually; data flows between systems are understood.	☐
		Best: Data classification and location are linked to risk assessment; data sovereignty and compliance requirements are actively monitored.	☐

Standard 3: Asset Importance

The organisation identifies and prioritises assets that support critical functions using a risk-based approach.

Process requirement	Description	Rating	
3.3 Secure baseline configuration	Default passwords and settings on routers, firewalls, and key systems have been changed and hardened (securely configured)	**Insufficient:** Default passwords and settings on internet equipment, firewalls, and key systems have been changed and hardened (securely configured), e.g., not using the out-of-the box settings.	☐
		Baseline: Defaults have been changed on all key systems; basic hardening has been applied (documented in IT setup records). For example, default passwords on routers and systems have been changed, and basic security settings have been applied and written down when systems were set up.	☐
		Better: Hardening is applied consistently using checklists or baselines; configurations are periodically reviewed.	☐
		Best: Configuration compliance is measured (e.g., via vulnerability scans or audits); deviations trigger remediation.	☐

Standard 3: Asset Importance

The organisation identifies and prioritises assets that support critical functions using a risk-based approach.

Process requirement	Description	Rating	
3.4 Software control	Only approved, supported software is installed on organisation devices	**Insufficient:** Staff can install software freely; unapproved applications are present.	☐
		Baseline: Approved software list exists; installation permissions are restricted to IT or practice manager or delegate. For example, the organisation or IT provider keeps a list of approved software, and only the IT provider or a nominated person can install new applications on organisation devices.	☐
		Better: Software approval process is standardised; periodic audits confirm compliance.	☐
		Best: Software inventory is tracked; unauthorised software installation rate is measured and acted upon.	☐

Standard 4: Secure Configuration of Software

The organisation ensures that systems are configured securely, following vendor guidance and best practice.

Process requirement	Description	Rating	
4.1 Vendor guidance followed	The organisation reviews vendor guidance and best practice when setting up new systems (no defaults)	**Insufficient:** Systems are set up using defaults; vendor guidance is not consulted.	☐
		Baseline: Vendor security guidance is reviewed and applied during setup; documented in implementation records. For example, when a new system is set up, the organisation or IT provider checks the supplier's security guidance and confirms that recommended security settings are used instead of defaults.	☐
		Better: Security configuration is part of a standard implementation process; configurations are validated before go-live.	☐
		Best: Configuration effectiveness is tested (e.g., via security assessment or penetration test); results inform future implementations.	☐

Standard 4: Secure Configuration of Software

The organisation ensures that systems are configured securely, following vendor guidance and best practice.

Process requirement	Description	Rating	
4.2 Unnecessary services disabled	Unnecessary services, insecure ports, and protocols are disabled on key systems	**Insufficient:** Unknown; configuration has not been assessed.	☐
		Baseline: Key systems (e.g., PMS, remote access, patient portals) have been reviewed; only functionality that the organisation uses is turned on where practical. For example, key systems have been checked to ensure only necessary features are turned on, reducing exposure to security risks.	☐
		Better: Hardening standards[2] are applied consistently; reviewed as part of routine maintenance.	☐
		Best: Hardening compliance is measured (e.g., via automated scans); gaps trigger remediation workflow.	☐

[2] Hardening standards are guidelines and best practices designed to secure systems, applications, and networks by reducing vulnerabilities and minimising the attack surface.

Standard 4: Secure Configuration of Software

The organisation ensures that systems are configured securely, following vendor guidance and best practice.

Process requirement	Description	Rating	
4.3 Configuration / setup change control	Changes to system setup or installation are agreed, documented and reviewed	**Insufficient:** Updates are applied without review.	☐
		Baseline: All changes are approved by the responsible party prior to updates being applied. For example, changes to how systems are set up are agreed by the responsible person at the organisation before updates are applied.	☐
		Better: Change control process includes organisation review and approval process.	☐
		Best: Checks are in place to ensure key systems are still set up as agreed and IT tooling is in place to alert if important settings change (externally facing systems).	☐

Standard 4: Secure Configuration of Software

The organisation ensures that systems are configured securely, following vendor guidance and best practice.

Process requirement	Description	Rating	
4.4 Configuration audits	The practice periodically audits key system configurations against agreed baseline standards	**Insufficient:** No audits conducted; configurations are unknown.	☐
		Baseline: Annual configuration review is conducted by IT provider; findings are documented. For example, once a year, the IT provider reviews system settings to confirm they still meet settings the organisation has agreed with its IT provider and document the findings.	☐
		Better: Configuration audits are scheduled routinely (e.g., annually or after major changes); results are acted upon.	☐
		Best: Audit frequency, findings, and remediation time are tracked; used to refine baselines and processes.	☐

Standard 5: Patching

The organisation ensures that security updates are applied promptly to protect systems from known vulnerabilities.

Process requirement	Description	Rating	
5.1 Operating system patching (regular maintenance of systems)	All servers and workstations apply critical security updates regularly (e.g., at least monthly)	**Insufficient:** Patching (e.g. system updates) is ad-hoc; some devices are months behind.	☐
		Baseline: Documented patch schedule exists; critical patches are applied within an agreed timeframe (e.g., 30 days). For example, there is a written agreement that security updates are applied regularly, such as monthly, and critical updates are not left for long periods. All computers and servers that handle patient information are supported and receive security patches.	☐
		Better: Patching is automated where possible; compliance is monitored; exceptions are tracked and managed.	☐
		Best: Patch compliance rates are measured and reported; time to patch critical vulnerabilities is tracked.	☐

Standard 5: Patching

The organisation ensures that security updates are applied promptly to protect systems from known vulnerabilities.

Process requirement	Description	Rating	
5.2 Anti-virus and anti-malware	Anti-virus/anti-malware is installed, active, and updating on all relevant devices	**Insufficient:** Some devices lack protection; updates are inconsistent.	☐
		Baseline: All devices have active, updating protection; definitions are current, e.g. all organisation computers have active protection (like Windows Defender) installed, and updates happen automatically without staff needing to manage them.	☐
		Better: Endpoint protection is centrally managed; alerts are monitored and acted upon.	☐
		Best: Protection effectiveness is measured (e.g., detection rates, false positives); tool performance informs purchasing decisions.	☐

Standard 5: Patching

The organisation ensures that security updates are applied promptly to protect systems from known vulnerabilities.

Process requirement	Description	Rating	
5.3 Application patching	The organisation has a process to review and apply updates to key applications (e.g., PMS, browsers, remote access tools)	**Insufficient:** Application updates are inconsistent or delayed.	☐
		Baseline: Key applications are updated regularly; process is documented in IT support agreement e.g. important software like the PMS and internet browsers are kept up to date as part of routine IT maintenance, and this is written into support arrangements.	☐
		Better: Application patching is tracked alongside operating system (OS) patching; embedded in routine maintenance.	☐
		Best: Application patch compliance is measured; vulnerabilities in unpatched applications are tracked and prioritised.	☐

Standard 5: Patching

The organisation ensures that security updates are applied promptly to protect systems from known vulnerabilities.

Process requirement	Description	Rating	
5.4 Legacy software management	Legacy or unsupported software is identified and replaced before support ends	**Insufficient:** Unsupported software remains in use indefinitely.	☐
		Baseline: Unsupported software is identified; replacement or mitigation plan is documented e.g. the organisation knows which software is no longer supported or receiving updates and has a written plan to replace it or manage the risk safely.	☐
		Better: Lifecycle planning prevents use of unsupported software; proactive replacement before end-of-support.	☐
		Best: Legacy software exposure is quantified (e.g., number of systems, risk level); reported to governance.	☐

Standard 6: Multi-factor Authentication (MFA)

The organisation uses multi-factor authentication (MFA) to strengthen access controls and protect against credential theft.

Process requirement	Description	Rating	
6.1 MFA for remote access and cloud	MFA is enabled wherever available for remote access and cloud services	**Insufficient:** MFA is not used; single-factor (password only) authentication is standard.	☐
		Baseline: MFA is enabled for remote access and cloud services (e.g., email, patient portal admin, hosted PMS access). For example, staff need both a password and a second step (such as a unique code or app prompt) to access email or systems from outside the organisation.	☐
		Better: MFA is required for all remote and privileged access; no exceptions without documented risk acceptance.	☐
		Best: MFA adoption and effectiveness are measured (e.g., coverage rate, bypass requests); gaps are closed.	☐

Standard 6: Multi-factor Authentication (MFA)

The organisation uses multi-factor authentication (MFA) to strengthen access controls and protect against credential theft.

Process requirement	Description	Rating	
6.2 MFA for critical systems	MFA is used for access to critical systems (e.g. PMS, patient portal admin, email admin)	**Insufficient:** MFA is not used.	☐
		Baseline: MFA is enabled on systems where technically feasible, e.g. where possible, systems like the PMS or patient portal admin accounts require a second login step in addition to a password.	☐
		Better: MFA is enforced as standard for all systems that store or process clinical information, as well as all administrative and elevated-privilege accounts.	☐
		Best: MFA coverage for critical systems is tracked; incident rates for MFA protected vs unprotected accounts are compared.	☐

Standard 6: Multi-factor Authentication (MFA) The organisation uses multi-factor authentication (MFA) to strengthen access controls and protect against credential theft.			
Process requirement	**Description**	**Rating**	
6.3 MFA user support	Staff understand how to use MFA and know what to do if they lose their authentication device	**Insufficient:** Staff are confused or frustrated by MFA; no clear support process.	☐
		Baseline: Staff receive MFA training at set up; clear support process exists (who to call, how to reset). For example, staff are shown how to use MFA when it is set up, and know who to contact if they lose their phone or cannot log in.	☐
		Better: MFA support is embedded in induction and ongoing training; self-service options are available where practical.	☐
		Best: MFA support metrics are tracked (e.g., reset requests, time to resolution); used to improve user experience and training.	☐

Standard 6: Multi-factor Authentication (MFA) The organisation uses multi-factor authentication (MFA) to strengthen access controls and protect against credential theft.			
Process requirement	**Description**	**Rating**	
6.4 MFA coverage review	MFA is reviewed and updated as new services or access points are added	**Insufficient:** MFA coverage is static; new systems may lack MFA.	☐
		Baseline: MFA requirements are part of new system assessment; gaps are identified and addressed e.g. when a new system is introduced, someone checks whether MFA is available and enables it if possible.	☐
		Better: MFA coverage is reviewed routinely (e.g., annually or when systems change); gaps trigger action.	☐
		Best: MFA gap analysis is conducted and reported; coverage percentage is tracked over time.	☐

Standard 7: Detect Unusual Behaviour

The organisation has processes in place to detect and respond to unusual or suspicious activity that may indicate a cyber security incident.

Process requirement	Description	Rating	
7.1 Log review	Logs or alerts from key systems (e.g., security tools, PMS hosting, email provider) are reviewed when something unusual is reported	**Insufficient:** Logs are not reviewed; unusual activity goes unnoticed.	☐
		Baseline: IT provider or security tools review logs reactively when an issue is reported; process is documented. For example, if something unusual happens, the IT provider checks system or email records of activity to help understand what occurred and what action is needed.	☐
		Better: Logs are reviewed proactively (e.g., weekly or monthly); key events are monitored (e.g., failed logins, unusual access times).	☐
		Best: Log review frequency, alert volume, and response times are measured; anomalies trigger automated alerts.	☐

Standard 7: Detect Unusual Behaviour

The organisation has processes in place to detect and respond to unusual or suspicious activity that may indicate a cyber security incident.

Process requirement	Description	Rating	
7.2 Monitoring	The organisation has basic monitoring to detect unusual activity (e.g., multiple failed logins, unusual access times)	**Insufficient:** No monitoring; reliance on user reports only.	☐
		Baseline: Basic monitoring is in place (e.g., via endpoint protection, email gateway, or PMS hosting provider). For example, basic alerts are in place to flag things like repeated failed logins or suspicious email activity.	☐
		Better: Monitoring is standardised across key systems; alerts are triaged and acted upon.	☐
		Best: Monitoring effectiveness is measured (e.g., false positive rate, time to detection); tuning is ongoing.	☐

Standard 7: Detect Unusual Behaviour

The organisation has processes in place to detect and respond to unusual or suspicious activity that may indicate a cyber security incident.

Process requirement	Description	Rating	
7.3 Alerts and notifications	IT provider or security tools alert the organisation to suspicious activity or anomalies	**Insufficient:** No alerts configured or received.	☐
		Baseline: Alerts are configured; the organisation knows how to receive and interpret them. For example, the organisation knows how alerts will be received (such as email or phone call) and who should respond when something looks suspicious.	☐
		Better: Alert thresholds and escalation paths are defined and tested; alerts integrate with incident response process.	☐
		Best: Alert metrics are tracked (volume, type, time to acknowledge); used to refine detection rules.	☐

Standard 7: Detect Unusual Behaviour

The organisation has processes in place to detect and respond to unusual or suspicious activity that may indicate a cyber security incident.

Process requirement	Description	Rating	
7.4 Staff awareness of detection	Staff know how to recognise, and report suspected incidents (ransomware, suspicious emails, lost devices)	**Insufficient:** Staff unaware; incidents go unreported.	☐
		Baseline: Staff know how to report; basic awareness training provided. For example, staff are trained to recognise common warning signs (phishing emails, ransomware messages, lost devices) and know how to report them.	☐
		Better: Reporting is normalised; staff receive feedback when they report (e.g., "thank you, this was malicious" or "false alarm, but good catch").	☐
		Best: Reporting rates and quality are measured; correlated with incident outcomes to refine training.	☐

Standard 8: Least privilege

The organisation ensures that users have only the access they need to perform their role, minimising the risk of unauthorised access or misuse.

Process requirement	Description	Rating	
8.1 Unique user accounts	Every staff member has their own unique login for clinical and business systems; no shared accounts	**Insufficient:** Shared accounts are common (e.g., a "Reception" or "Nurse" account).	☐
		Baseline: All staff have unique logins; shared accounts have been eliminated or documented as exceptions. For example, each staff member logs in using their own name, and shared logins like “Reception” are no longer used unless formally approved.	☐
		Better: Unique accounts are enforced by policy and technical controls; new staff cannot start without their own account. A formal process to grant, review, and remove user access is in place and largely complied with.	☐
		Best: Account provisioning and de-provisioning compliance is tracked; shared account usage (if any) is monitored and minimised.	☐

Standard 8: Least privilege

The organisation ensures that users have only the access they need to perform their role, minimising the risk of unauthorised access or misuse.

Process requirement	Description	Rating	
8.2 Role based access	Staff access is limited to what they need for their role	**Insufficient:** Access is broad; most staff have more access than needed.	☐
		Baseline: Roles are defined in systems like the PMS and applied at user creation; access aligns with job function. For example, reception staff, nurses, and doctors have different access levels in systems based on their job role.	☐
		Better: Role-based access is applied consistently across all systems; roles are reviewed when duties change.	☐
		Best: Access creep is measured (e.g., via periodic access reviews); excess permissions are identified and removed.	☐

Standard 8: Least privilege The organisation ensures that users have only the access they need to perform their role, minimising the risk of unauthorised access or misuse.			
Process requirement	**Description**	**Rating**	
8.3 Account lifecycle management	Accounts are promptly disabled when staff leave or change roles	**Insufficient:** Delays are common; inactive accounts may remain active for weeks or months.	☐
		Baseline: Account disabling is documented in an offboarding checklist; completed within 24 hours of departure. For example, when someone leaves the organisation, disabling their system access is part of the offboarding checklist and happens within one working day.	☐
		Better: Account lifecycle is managed systematically; automated alerts flag overdue reviews or stale accounts.	☐
		Best: Time to disable departing staff accounts is tracked; inactive accounts are reported and acted upon.	☐

Standard 8: Least privilege The organisation ensures that users have only the access they need to perform their role, minimising the risk of unauthorised access or misuse.			
Process requirement	**Description**	**Rating**	
8.4 Privileged account management	Administrative or privileged accounts are only used when necessary and closely monitored	**Insufficient:** Privileged accounts are used routinely for daily tasks.	☐
		Baseline: Privileged accounts are separated from standard user accounts; use is restricted to IT/admin tasks. For example, accounts with extra permissions are only used for IT tasks and not for everyday work like checking email.	☐
		Better: Privileged access is logged and reviewed; elevation requires justification.	☐
		Best: Privileged account usage metrics are tracked (e.g., frequency, duration, anomalies); used to refine controls.	☐

Standard 9: Data Recovery

The organisation has robust backup and recovery processes to ensure critical systems and data can be restored following an incident.

Process requirement	Description	Rating	
9.1 Regular backups	The organisation takes regular backups of critical systems (e.g., PMS and key files) and knows where backups are stored	**Insufficient:** Backups are assumed but not verified; location and schedule unclear.	☐
		Baseline: Backup schedules, locations, and retention periods are documented (e.g., in IT support agreement). For example, the organisation knows when backups run, where they are stored, and how long they are kept, and this information is written down.	☐
		Better: Backups are automated and monitored; backup success is confirmed regularly (e.g., weekly automated reports).	☐
		Best: Backup success rates, storage usage, and age of oldest successful backup are measured; reported to governance.	☐

Standard 9: Data Recovery

The organisation has robust backup and recovery processes to ensure critical systems and data can be restored following an incident.

Process requirement	Description	Rating	
9.2 Ransomware-resistant backups:	Backups are protected from ransomware (e.g., offline, immutable, or via secure hosted service)	**Insufficient:** Backups are on the same network as live systems; vulnerable to ransomware.	☐
		Baseline: Backups are segregated (offline, air-gapped, or immutable cloud storage). For example, backups are stored separately from everyday systems (e.g. on a separate hard drive that is not always plugged in) so they can't be encrypted or deleted during a ransomware attack.	☐
		Better: Ransomware resilience is tested; backup isolation is verified as part of routine checks.	☐
		Best: Backup resilience is assessed using defined criteria; test results are documented and reviewed.	☐

Standard 9: Data Recovery The organisation has robust backup and recovery processes to ensure critical systems and data can be restored following an incident.			
Process requirement	**Description**	**Rating**	
9.3 Restore testing	Data recovery is tested at agreed intervals for all critical systems, including all cloud-hosted and SaaS services with results confirmed by the organisation and IT provider	**Insufficient:** Data recovery has not been tested; the ability to restore systems and data is assumed.	☐
		Baseline: Data recovery has been tested at least once for each critical system, and the outcome has been confirmed with the IT provider. For example, at least once, the organisation has confirmed with the IT provider that data can actually be restored from backups.	☐
		Better: Data recovery is tested at planned intervals (e.g. annually) for all critical systems. Test results, issues and follow-up actions are recorded and reviewed by organisation leadership.	☐
		Best: Recovery tests are carried out at defined intervals using realistic scenarios. Recovery time and data loss are measured against agreed objectives, and lessons learned are used to improve recovery arrangements.	☐

Standard 9: Data Recovery The organisation has robust backup and recovery processes to ensure critical systems and data can be restored following an incident.			
Process requirement	**Description**	**Rating**	
9.4 Business continuity plan	The organisation has a simple written business continuity plan for operating during IT outages	**Insufficient:** No plan exists; response is ad-hoc.	☐
		Baseline: A short plan exists covering how to see urgent patients, access key information, and contact IT support during an outage. For example, a short, written one page plan explains how the organisation will operate during an IT outage, including seeing urgent patients and contacting IT support.	☐
		Better: Business continuity plan is tested (e.g., via tabletop exercise); staff know their roles.	☐
		Best: Plan effectiveness is measured (e.g., exercise outcomes, actual outage response); lessons learned drive plan updates.	☐

Standard 10: Response Planning

The organisation has documented processes and contacts in place to respond effectively to cyber security incidents.

Process requirement	Description	Rating	
10.1 Incident response guide	The practice has a one-page incident response guide (e.g., who to call, first steps, what not to do)	**Insufficient:** No guide exists; response is reactive and uncoordinated.	☐
		Baseline: A simple, written incident response guide is available (posted or easily accessible); covers ransomware, privacy breach, lost device. For example, a one-page guide is available showing who to call, what to do first, and what not to do if there is a cyber incident.	☐
		Better: Incident response guide is tested (e.g., via tabletop exercise); updated based on lessons learned or new threats. Business continuity plans (BCP) are aligned with risk registers so that BCP / disaster recovery (DR) plans prioritise critical / external facing systems first.	☐
		Best: Incident response metrics are tracked (time to detect, time to contain, cost of incidents); used to refine the response process.	☐

Standard 10: Response Planning

The organisation has documented processes and contacts in place to respond effectively to cyber security incidents.

Process requirement	Description	Rating	
10.2 Technical support contracts	The organisation knows who will provide technical help in a serious cyber incident (e.g., IT provider, vendor, insurer, specialist)	**Insufficient:** No clear contacts; staff would have to search for help in a crisis.	☐
		Baseline: Key contacts are documented (e.g., IT provider emergency line, PMS vendor support, cyber insurance claims contact). For example, emergency contact details for IT support, the PMS vendor, and cyber insurance are written down and easy to find.	☐
		Better: Contact list is tested and kept current; roles and escalation paths are clear (who decides what, when to escalate).	☐
		Best: Response time and availability of support contacts are measured; service level expectations are reviewed annually.	☐

Standard 10: Response Planning The organisation has documented processes and contacts in place to respond effectively to cyber security incidents.			
Process requirement	**Description**	**Rating**	
10.3 Incident exercises	The organisation has conducted at least one cyber incident tabletop exercise (scenario walk-through) in the last three years	**Insufficient:** No cyber incident exercises conducted.	☐
		Baseline: At least one tabletop exercise has been conducted; attendees included practice manager, IT contact, and key clinical staff. For example, the organisation has walked through a realistic cyber incident scenario with key staff to discuss what actions would be taken.	☐
		Better: Exercises are routine (e.g., annually); scenarios vary (ransomware, privacy breach, prolonged outage).	☐
		Best: Exercise outcomes are measured (e.g., time to key decisions, gaps identified, actions completed); used to improve response capability.	☐

Standard 10: Response Planning The organisation has documented processes and contacts in place to respond effectively to cyber security incidents.			
Process requirement	**Description**	**Rating**	
10.4 Privacy and regulatory response	The incident response plan includes privacy notification requirements and contact details for PHO, insurer, and privacy officer	**Insufficient:** Privacy breach response is unclear; statutory notification requirements not documented.	☐
		Baseline: Privacy breach notification steps are documented (e.g., who to notify, timeframes, escalation to Privacy Commissioner if required). For example, the incident plan explains who is responsible for privacy notifications and when external agencies need to be informed.	☐
		Better: Privacy response is integrated with technical response; tested via scenario exercise.	☐
		Best: Privacy breach response times and compliance with notification requirements are tracked; reviewed after each incident.	☐