NZ Medical Practice Cyber & Privacy Readiness Checklist

This checklist is for practice managers, clinical leads, and partners at New Zealand GP and specialist practices. It is built around the controls clinical IT environments actually need: the ones that protect patient information, keep the clinical system available during a ransomware incident, and produce defensible evidence for an Office of the Privacy Commissioner inquiry.

You will get a printable checklist covering twelve control areas: the Health Information Privacy Code, Privacy Act 2020 in a clinical setting, indici, Medtech, and Healthlink integration security, patient portal MFA, clinical-grade uptime, secure messaging, ransomware exposure scenarios, breach notification, staff training, BYOD policy, backup testing, and after-hours support continuity.

Why this matters for NZ medical practices

Health information has the strictest privacy regime in New Zealand. The Health Information Privacy Code 2020 (HIPC) sits over the Privacy Act 2020 and applies thirteen Health Information Privacy Rules to anyone collecting, holding, using, or disclosing health information. The HIPC covers GPs, specialists, allied health, pharmacies, and any vendor that processes health data on a practice's behalf. The Office of the Privacy Commissioner is the regulator, and the breach notification threshold is the same as the rest of the Privacy Act: any breach likely to cause serious harm must be notified as soon as practicable.

Clinical systems in New Zealand have a small and well-known set of vendors: indici, Medtech (Evolution and 32), Profile, MyPractice, and Houston for specialist groups. They all integrate with Healthlink for secure messaging and referrals. They all integrate with the National Health Index (NHI) and with eRx for prescribing. The result is that a practice's data is rarely in one place. A patient record exists in your PMS, fragments exist in your secure messaging archive, lab results sit in your Healthlink mailbox, and clinical correspondence may be in Microsoft 365 or Google Workspace.

Practices have been on the wrong end of cyber incidents in the past few years. Pinnacle Midlands Health Network and Te Whatu Ora Waikato are the publicly disclosed examples that practice managers most often raise. The lesson from both is consistent: the path through the network mattered far more than the initial entry point. Once an attacker had a foothold, the lack of segmentation, the shared service accounts, and the patch lag combined to make the blast radius wide.

And there is the operational side. A clinic that loses access to its PMS during a working day cannot prescribe, cannot bill, and cannot safely cover after-hours triage. Cyber resilience for a practice is not only about confidentiality. It is about continuity of care.

Get the checklist

Printable PDF covering twelve control areas across HIPC, clinical software, and continuity of care.

The Checklist

What the checklist covers

Twelve control areas, each one grounded in a specific NZ rule, a specific clinical workflow, or a specific failure mode.

1. Health Information Privacy Code 2020 (HIPC)

The HIPC's thirteen Health Information Privacy Rules govern collection, use, disclosure, storage, retention, and access for any health information a practice holds. Rule 5 (storage and security) is the rule most often cited in OPC findings against practices. It requires reasonable security safeguards against loss, misuse, unauthorised access, and disclosure.

The checklist maps each HIPC rule to a concrete control: where Rule 5 becomes "MFA on every clinical login", where Rule 9 (retention) becomes "ten-year minimum retention for clinical notes with documented destruction process", and where Rule 11 (disclosure) becomes "audit logging on every export from the PMS".

2. Privacy Act 2020 in a clinical setting

The Privacy Act 2020 sits underneath the HIPC and provides the notifiable breach mechanism. A notifiable privacy breach involving health information is treated by the OPC as a serious matter, and the OPC's published case notes show that lack of basic controls (no MFA, no access review, shared passwords) is treated as an aggravating factor.

The checklist gives you the notification decision tree, the OPC online form fields, and the evidence to capture during the incident so the eventual notification is defensible.

3. indici, Medtech, Profile, MyPractice security

Each PMS has its own security model. indici is delivered as a cloud service with role-based access and tenant-level audit. Medtech Evolution and Medtech 32 have different deployment topologies (cloud and on-premises). Profile and MyPractice each have their own approach to user roles and audit trails. The questions to ask are the same regardless of vendor: who has Administrator, what is logged, how long are logs retained, what is the MFA story, and what is the data location.

The checklist gives you the vendor-question template, the typical answers, and the gaps to close on each platform.

4. Healthlink and secure messaging

Healthlink is the de facto secure messaging backbone for New Zealand primary care, used for referrals, lab results, and specialist correspondence. The Healthlink endpoint at the practice is usually a small server or a workstation running the Healthlink client. That endpoint is also a privacy boundary: anything reaching the Healthlink mailbox is sensitive health information, and the mailbox archive is often retained for years.

The checklist covers Healthlink endpoint hardening, the access controls on the Healthlink share, archive retention alignment with the rest of your record retention, and the failure mode of a Healthlink endpoint that has been silently offline for days.

5. Patient portal MFA

ManageMyHealth, Health365, Indici Patient Portal, Konnect NET, and the various PMS-specific portals all expose patient self-service. They also expose a patient's clinical record to anyone who can compromise the patient's login. SMS-based MFA on patient portals is now standard but is not universal, and most portals support stronger options (authenticator app, passkey) that are not enabled by default.

The checklist covers what to enable, what to recommend to patients, and the policy stance on portal account recovery (which is itself a frequent attack path).

6. Clinical-grade uptime and continuity of care

A clinic offline for half a day is not just a productivity problem. It is a clinical risk: deferred prescriptions, deferred triage, deferred follow-up. The continuity question is not "do we have backups". It is "if the PMS is unavailable for four hours during a Monday morning, what is our plan, and have we tested it".

The checklist gives you a continuity-of-care worksheet: which workflows can move to paper, which lab results are most time-critical, who has authority to defer non-urgent appointments, and the trigger conditions for activating an alternate prescribing channel.

7. Ransomware exposure for NZ practices

The realistic ransomware path into a clinic is well understood. Phishing email or stolen credential. Lateral movement through a flat network. Privilege escalation via a service account with too much access. Encryption of the file server, the PMS database (if on-prem), and the backup target if it is reachable from the production network. The fix is segmentation, immutable backup, EDR with active response, and managed identity hygiene.

The checklist covers the four controls that consistently bound the blast radius, and the two controls (immutable backup and EDR with response) that most often turn a catastrophic incident into a recoverable one.

8. Ministry of Health and Te Whatu Ora guidance

The Ministry of Health and Te Whatu Ora publish guidance on health sector cyber resilience, including the Health Information Standards Organisation (HISO) standards. HISO 10029 covers health information security, and HISO 10064 covers identity and access management for health. These are the standards that PHO contracts and DHB-era service agreements typically reference.

The checklist maps the HISO standards to a practitioner-level set of controls so a practice manager can answer "yes, we comply" with the evidence to back it up.

9. Breach notification to the OPC

A notifiable privacy breach involving health information has to be reported to the OPC and to affected individuals as soon as practicable, generally taken to mean within seventy-two hours

where harm is clear. The OPC has a published online notification form. The information you need to provide (what was breached, how many people, what mitigation, what notification to individuals) is best captured during the incident, not reconstructed later.

The checklist gives you a one-page incident capture sheet aligned with the OPC form, ready to use in the moment.

10. Staff training and clinical workflows

Most breaches involve a person clicking, forwarding, sharing, or storing something they should not have. Training that says "do not click suspicious links" does not change behaviour. Training that walks through the actual scenarios (a fake DHB request, a fake referral attachment, a fake Healthlink notification) does.

The checklist covers the cadence (six-monthly minimum), the content (scenario-based, role-specific), and the evidence of completion that an OPC inquiry or insurer will look for.

11. BYOD policy for clinical staff

GPs, locums, and on-call specialists routinely access PMS, Healthlink, and email from personal devices. Without a documented BYOD policy and a technical control set (conditional access, app protection, no save-to-device for clinical attachments), every personal phone is an uncontrolled copy of patient data.

The checklist gives you a BYOD policy template aligned with HIPC, the Microsoft 365 conditional access policies that enforce it, and the offboarding sequence when a locum's engagement ends.

12. Backup testing and after-hours support continuity

A backup that has never been restored is not a backup. For a clinical environment the test cadence should be at least quarterly, the restore should target a representative PMS dataset and a Healthlink archive, and the timing should be recorded against an agreed Recovery Time Objective. After-hours support continuity is the same question for the on-call workflow: if the after-hours service cannot reach the PMS, do they have read-only access to a recent extract, and is that extract refreshed daily.

The checklist gives you the test plan, the documentation template, and the after-hours fallback options used by practices we work with.

How Belton Helps

If you want the controls implemented, not just listed

We work with NZ GP and specialist practices on clinical IT, HIPC alignment, and continuity of care.

Managed IT

End-to-end IT management for medical practices: identity, clinical endpoints, Healthlink, email, file storage. We run the controls and produce the evidence HIPC compliance asks for.

Managed IT →

Security Operations

Twenty-four-hour monitoring of your tenant, your endpoints, and your clinical software access. We see the unusual login at two in the morning before it becomes a breach.

Security Operations →

Compliance Support

HIPC and Privacy Act 2020 readiness for practices. We help you produce the documentation, train your team, and prepare a breach response that holds up under OPC review.

Compliance →

> **Want a one-on-one review?**
>
> Book a 30-minute Discovery and Security Session with one of our senior engineers. We will review your current setup, where the regulatory exposure sits, and what would change first.
>
> outlook.office.com/book/BeltonDiscoveryandSecuritySession@belton.co.nz
>
> **Belton IT Nexus** · Level 3, 101 Carlton Gore Road, Newmarket, Auckland 1023 · 09 974 2379 · support@belton.co.nz