Te Puke Medical Centre

Privacy and Health Information Security Policy

Policy summary

This Privacy and Health Information Security Policy outlines the responsibilities and obligations of all staff and associated professionals at Te Puke Medical Centre regarding the management of patients' health information. The policy ensures that information about patients, including any details related to their health and treatment, is collected, used, stored, and disclosed in accordance with the Privacy Act 2020 and the Health Information Privacy Code 2020 (HIPC).

From 1 May 2026, the HIPC includes Information Privacy Principle 3A (IPP3A), which introduces a new requirement to inform patients when their health information is collected indirectly (that is, from sources other than the patient themselves). This policy has been updated to reflect that change.

The Privacy Officer, designated as the Practice Manager oversees adherence to these standards and is the key point of contact for any privacy-related matters within the organisation.

This policy applies to all kaimahi/staff employed by Te Puke Medical Centre, and to all visiting health professionals, contractors, and students undertaking training or education with the organisation.

Purpose

The purpose of this policy is to ensure that Te Puke Medical Centre complies with:

- The Privacy Act 2020, which promotes and protects the privacy of personal information; and
- The Health Information Privacy Code 2020, including IPP3A, which sets specific rules for the collection, use, storage, disclosure, and notification of health information.

Policy principles

The Privacy Officer is responsible for ensuring that Te Puke Medical Centre complies with the Health Information Privacy Rules, including:

1. Purpose of collection of health information
2. Source of health information
3. Collection of health information from the individual (IPP3) | 3A. Notification of indirect collection of health information (IPP3A)
4. Manner of collection of health information
5. Storage and security of health information
6. Access to health information
7. Correction of health information
8. Accuracy of health information
9. Retention of health information
10. Limits on use of health information
11. Limits on disclosure of health information
12. Disclosure of health information outside New Zealand
13. Unique identifiers

Collection of health information

Direct collection (IPP3)

When collecting health information directly from patients, staff must:

- Collect only information necessary for providing care or for another lawful purpose
- Inform patients:
    - why the information is being collected
    - who will have access to it
    - that they have the right to access and request correction of their information

Indirect collection (IPP3A – effective 1 May 2026)
Te Puke Medical Centre may also receive health information about patients from other sources, including but not limited to:

- Hospital discharge summaries
- Laboratory or radiology results
- Specialist letters
- Shared care records
- PHO, NGO, or other provider communications
- Digital tools or systems that receive data from external sources (including AI-enabled tools)

When health information is collected indirectly, the practice must take reasonable steps to inform the patient.

Patients must be informed:

- What information has been collected
- The purpose for which it was collected
- Who the information may be shared with
- Their rights to access and request correction of the information

How patients are informed
Notification may occur through one or more of the following:

- The practice privacy statement (website, enrolment material, or patient information)
- Patient portal messages or notifications
- Verbal explanation where appropriate (e.g. following hospital discharge)

The method used must be reasonable in the circumstances, considering:

- The sensitivity of the information
- The context in which it was received
- The practicality of providing individual notification

Use of health information
Before using health information, staff must:

- Take reasonable steps to ensure the information is accurate and up to date
- Use the information only for the purpose for which it was collected, unless:
    - the patient has consented to another use; or
    - an exception under the HIPC applies

Staff must consult the Privacy Officer before using health information without patient consent.

Storage and security of health information

Te Puke Medical Centre ensures that all health information is stored securely and protected from unauthorised access, use, modification, or disclosure.
This includes:

- Secure electronic systems and individual user logins
- Secure handling of transferred information
- Retention of health records for a minimum of 10 years from last treatment
- Secure destruction of information when no longer required

Access and correction
Patients are entitled to:

- Request confirmation of whether the practice holds information about them
- Access their health information (unless lawful grounds for withholding apply)
- Request correction of their health information

Staff must assist patients promptly with access and correction requests.

Disclosure of health information
Health information must not be disclosed without patient consent unless permitted or required under the HIPC or other legislation (e.g. for treatment, serious threat to life or health, child protection, or statutory reporting obligations).

The Privacy Officer must be consulted before any disclosure without consent.

Roles and responsibilities
Privacy Officer
The Privacy Officer is responsible for:

- Maintaining this policy and associated procedures
- Ensuring staff are trained in privacy obligations, including IPP3A
- Keeping up to date with legislative changes and briefing staff accordingly
- Overseeing responses to privacy complaints and breaches
- Ensuring patient notification requirements for indirect collection are met

All staff
All staff are responsible for:

- Understanding and complying with this policy
- Protecting patient privacy in day-to-day work
- Escalating privacy concerns or incidents promptly

Privacy breaches
Privacy breaches that pose, or are likely to pose, a risk of serious harm must be reported to:

- Affected individuals; and

- The Privacy Commissioner

The Privacy Officer is responsible for assessing and managing privacy breaches in accordance with the Privacy Act 2020.

Training and awareness
All staff must receive:

- Privacy and HIPC training at induction
- Ongoing refresher training, including updates relating to IPP3A and indirect collection of health information

References
This policy is informed by, and should be read in conjunction with, the following legislation and guidance:

- Privacy Act 2020 (New Zealand)
- Health Information Privacy Code 2020 (HIPC), including, Information Privacy Principle 3 (Collection of health information from the individual) and Information Privacy Principle 3A (Notification of indirect collection of health information), effective 1 May 2026
- Office of the Privacy Commissioner (OPC) guidance on health information and patient notification obligations
- Royal New Zealand College of General Practitioners (RNZCGP) Foundation Standards – Privacy and information security indicators

Further guidance and updates may be issued by the Office of the Privacy Commissioner from time to time. The Privacy Officer is responsible for monitoring relevant updates and ensuring this policy remains current.