

## Patient Information and Records Practice Standard

### **Purpose**

The purpose of the patient information and records practice standard is to set minimum standards for podiatrists in creating and maintaining patient records and maintaining the privacy of patients' health information.

Patient records assist practitioners in providing safe, effective, and complete care and enable them to collaborate effectively with their colleagues and other health practitioners, in the interests of good patient care. They may also be used in forensic investigations and complaint resolution, and in quality review and audit processes.

The standards apply to patient records and health information regardless of the form in which it is held, or where, and covers paper-based and digital records.

### **Duty of patient care**

Practitioners have a responsibility to ensure safe practice and put their patients' interests first by maintaining accurate, time-bound and up-to-date patient records and protecting the confidentiality of a person's health information.

A person's health information is collected within the context of the practitioner-patient relationship - a partnership based on trust and respect which is focused on meeting the health needs and goals of that person. It is vital that practitioners maintain patient trust by treating all patient health information as sensitive and confidential.

[The Health and Disability Commissioner \(Code of Health and Disability Services Consumers' Rights\) Regulations 1996 \(the Code\)](#) provides that every consumer has the right to have services provided with reasonable care and skill that comply with legal, professional, ethical and other relevant standards and this includes treating patient information appropriately.

The Code provides that every person has the right to have services provided with reasonable care and skill that comply with legal, professional, ethical and other relevant standards and this includes treating patient information appropriately.

## Legislation

[The Privacy Act 2020](#) applies to any action taken and all personal information collected or held by a New Zealand entity, both inside and outside Aotearoa New Zealand; and to any action and all personal information collected or held by an overseas entity in the course of “*carrying on business*” in Aotearoa New Zealand.

Where the information concerns a person’s health, the [Health Information Privacy Code 2020](#) (HIPC) additionally applies, and has the same legal standing as the Privacy Act. Where the HIPC is mentioned in this document, the reference may also be to relevant parts of the Privacy Act.

The HIPC defines ‘*health information*’ in relation to an identifiable individual as:

- (a) Information about the health of that individual, including that individual’s medical history.
- (b) Information about any disabilities that an individual has, or had.
- (c) Information about any health or disability services that are being provided, or have been provided, to that individual.
- (d) Information provided by that individual in connection with the donation, testing, or examination, of any body part or bodily substance, of that individual.
- (e) Information about that individual which is collected prior to, or in the course of, and incidental to, the provision of any health or disability service to that individual.

Typically, in the podiatry context, a person’s health information is contained in the patient record, which also includes financial transactions associated with services that have been provided.

The *New Zealand Standard Health Records* (NZS 8153:2002) sets out the minimum requirements for the appropriate documentation and management of health records within public and private healthcare services in Aotearoa New Zealand.

The standards and guidance in this practice standard are principally based on the legal and professional obligations described in the Privacy Act and the HIPC, [the Health \(Retention of Health Information\) Regulations 1996](#) and the [NZS 8153:2002](#).

[On the record. A practical guide to health information privacy](#), published by the Office of the Privacy Commissioner, may also be a useful additional reference in this practice area.

## Components of the patient record

The patient record includes (but is not limited to):

- Completed patient questionnaires, including patient information required for administrative purposes, and medical history.
- Medical imaging, clinical photographs, and models.
- Clinical notes documenting assessments, diagnosis, recommendations for prevention of disease and promotion of health, and treatment offered and provided, or declined.
- Information and documents related to informed consent.

- Results or reports related to special tests or investigations.
- Digital information related to computer assisted restoration design and construction processes.
- Correspondence (or copies of) related to the person.
- Financial transactions.

## **Ownership of patient records**

While physical patient records (forms, computer systems etc.) are owned by the practice owner(s), people are entitled to access and seek correction of their health information and may request their records which may be transferred to them, subject to a small number of specific grounds for refusal outlined in sections 49 – 53 of the Privacy Act 2020. People do not have the right to take away original records (see standards 8 and 9).

## **Responsibilities for staff**

The HIPC holds a ‘health agency’ responsible for the actions of those working for it, whether paid or unpaid, except where the person was clearly working outside his or her authority or instructions. The term ‘health agency’ covers all providers of public or private health or disability services, podiatry practices included.

Therefore, practice owners are responsible for ensuring that staff understand and comply with the legal obligations of the HIPC, reflected in this practice standard. It is anticipated that staff briefing, or training would be necessary to enable staff to properly manage patient records and maintain the privacy of a person’s information.

## **Role of the Privacy Officer**

Section 201 of the Privacy Act requires a health agency to have at least one person acting as a “privacy officer”, whose responsibilities include:

- Encouraging the agency to comply with the information privacy principles in the Privacy Act and rules in the HIPC.
- Dealing with requests made to the agency under the Privacy Act and HIPC.
- Working with the Privacy Commissioner in relation to any investigations conducted under the Privacy Act in relation to that agency.
- Ensuring compliance by the health agency with the Privacy Act and the HIPC.

The person does not have to be dedicated only to information privacy issues. However, the responsibilities listed above do need to be included in the duties of at least one person within the podiatry practice.

The Privacy Act also requires all health agencies to have procedures to enable appropriate and timely management of complaints, and to designate a person to deal with complaints related to privacy issues. This person may be the privacy officer or another individual within the practice.

People are entitled to know of their right to complain directly to the Privacy Commissioner when they feel their privacy has been infringed.

## Practice Standards

The Patient Information and Records Practice Standard sets the minimum standards for the process of maintaining patient records and ensuring the privacy of health information, and are listed below:

1	You must create and maintain patient records that are comprehensive, time-bound and up to date, and that represent an accurate and complete record of the care you have provided.
2	You must collect a person's health information only for lawful purposes connected with your professional functions and activities.
3	You must take reasonable steps to ensure that a person or their representative is aware that health information is being collected, the purpose of collection, and the potential impact of not providing all the requested information.
4	You must collect health information in a manner which is lawful, and fair in the circumstances, and which does not intrude to an unreasonable extent on a person's personal affairs unnecessarily.
5	You must ensure security safeguards are in place to protect a person's health information.
6	You must give people access to their personal health information on request, and in the form the person prefers, when possible, except when withholding grounds contained in the Privacy Act 2020 apply.
7	You must take reasonable steps to correct a person's health information, on their request.
8	You must check that health information that is collected and recorded by someone else is accurate, up-to-date, and complete before using or disclosing it.
9	You must ensure that your patients' records are retained for a minimum of 10 years from the day following the last date on which care was provided, or the records are properly transferred.  Note: Under the <a href="#">Public Records Act 2005</a> patient records held by DHBs are considered public records, and may not be disposed of without the authorisation of the Chief Archivist.

10	You must only use health information for the purpose for which it was collected unless the person gives their permission for it to be used for another purpose, or another exception of the HIPC applies.
11	You must disclose health information only to the person concerned, or their representative unless the person or their representative authorises the disclosure, or another exception of the HIPC applies.
12	You must only disclose health information outside of Aotearoa New Zealand if you have taken reasonable steps to ensure the information is protected by acceptable privacy standards.
13	You must use unique identifiers only for the purpose of enhancing practice efficiency; and must not use the same identifier given by another body, with the exception of the person's NHI number.

## Privacy breach

A health information privacy breach in relation to health information held by an agency occurs when there is:

- (a) Unauthorised access to, or disclosure, alteration, loss or destruction of, the health information; or
- (b) An action that prevents the agency from accessing the information on either a temporary or permanent basis; **and**

includes any of these actions or things listed in (a) or (b) above whether or not the action or thing:

- (a) was caused by a person inside or outside the agency; or
- (b) is attributable in whole or in part to any action by the agency; or
- (c) is ongoing.

Privacy breaches often involve people's health information being accidentally lost or disclosed, for example, being emailed to the wrong person or a breach in system security.

## Notifiable privacy breach

A notifiable privacy breach means a privacy breach that it is reasonable to believe has caused serious harm to an affected individual or individuals or is likely to do so. When assessing whether a privacy breach is likely to cause serious harm you must consider the factors set out in [section 113 of the Privacy Act](#).

The Privacy Commissioner has an online tool called [NotifyUS](#) that is available to assist agencies in determining if a breach is notifiable and to guide agencies through the notification process. The Privacy Commissioner expects that agencies will use this tool.

If a privacy breach that meets the definition of a notifiable privacy breach in the Privacy Act 2020) occurs, you must:

- Report the breach to the Privacy Commissioner as soon as possible.
- Report the breach to the person/people concerned as soon as possible **unless** an exception in the Privacy Act 2020 applies.

**Reviewed September 2024**