Privacy Commissioner
Te Mana Mātāpono Matatapu

Health Information Privacy Code Fact Sheet 5

Storage, security, retention and disposal of health information

Health Information Privacy Code 2020

The Health Information Privacy Code (HIPC) regulates how health agencies (such as doctors, nurses, pharmacists, health insurers, Primary Health Organisations, the Ministry of Health, and Health New Zealand) collect, hold, use, and disclose health information about identifiable people.

Storage and security

One of the obligations that health agencies have when they hold health information is to keep that information secure.

Rule 5 of the Code requires health agencies to take 'reasonable security safeguards' to protect health information. This means keeping the information safe from loss, as well as from unauthorised access, use, modification or disclosure.

To comply with rule 5, agencies need to consider what risks there are for the health information they hold, plan to address those risks, and do whatever is necessary to carry it out.

Some areas that need to be considered when coming up with a security plan are:

- **Electronic** security – use of email, laptops and portable storage devices, and passwords.
- **Operational** security – confidentiality agreements with staff and contractors, document tracking and footprinting, and staff training.
- **Physical** security – entry controls, positioning of whiteboards and computer terminals, locked filing cabinets and storage rooms.

This list isn't exhaustive. Security is an ongoing obligation rather than a 'tick the box' exercise.

The greater the risk of a security breach and the more serious the potential consequences for people whose information is in danger, the higher the standard will be for a 'reasonable security safeguard'. We recommend that you seek advice on your security settings and vulnerabilities.

Retention

Health Act regulations require all health information held by providers to be retained for 10 years from the last encounter with the patient, unless transferred to another doctor or to the patient.

The Public Records Act also requires retention by public sector agencies. A Functional Disposal Authority lists how long each type of clinical record must be kept for and what must be done afterwards.

- Once the retention periods have passed, rule 9 of the Code says that health information should be disposed of, securely, unless the health agency has a lawful purpose to retain it.

Disposal

Health agencies need to be careful to dispose of patient records securely and effectively.

Where information is stored in a hard copy, such as paper records, disposal might include secure shredding or hiring a secure destruction contractor. Where information is stored electronically, such as in cloud-based storage, USBs or with a third-party provider, health agencies must ensure the records are permanently destroyed including in any back-up system or offsite storage.

Health Information Retention Policy

It can be complex to navigate the different legal rules and standards that deal with the retention of health information. Given this complexity,

we recommend that health agencies develop a health information retention policy. This policy should outline:

- the kinds of information you hold
- how long you are legally required to keep the different kinds of information
- when you will dispose of different kinds of information
- how you will dispose of the information.

Dealing with records after a clinician dies or ceases practice

When a sole trader clinician (such as a GP) ceases practice or dies, their patient records should either be:

- **transferred** to the new treating clinician
- **returned** to the patient or
- **held securely** in trust by another agency until one of the two things above can take place. The GP's Primary Health Organisation should be contacted to assist with the transfer or return of records.

Where the statutory retention period has ended, the records may be securely destroyed.

Where to get additional assistance

There are four other Health Information Privacy Code fact sheets that give an overview of how the Code works in practice.

For more detailed information, a copy of the Health Information Privacy Code is available privacy.org.nz

The Office of the Privacy Commissioner does not administer the Health Act regulations or the Public Records Act. If you have questions about how these rules applies to your health agency you should talk to your agency's privacy officer, a lawyer, or the Ministry of Health.

For enquiries, please ring the Office of the Privacy Commissioner on 0800 803 909 or email enquiries@privacy.org.nz