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 code regulates how health agencies (such as doctors, nurses, pharmacists, health insurers, hospitals, Primary Health Organisations, ACC and the Ministry of Health) collect, hold, use and disclose health information about identifiable individuals.

Storage and security

One of the obligations that health agencies take on 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, make a plan to address those risks and do what 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, passwords
- **operational** security – confidentiality agreements with staff and contractors, document tracking and footprinting, 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'**.

Retention and disposal

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. **The DHB General Disposal Authority** lists how long each type of clinical record must be kept for and what must be done afterwards.

Once the obligatory 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.

Dealing with records after a clinician dies or ceases practice

When a 'sole trader' clinician, such as a GP, dies or ceases practice, his or her patient records should be either:

- **transferred** to the new treating clinician
- **returned** to the patient or
- **held securely** in trust (for instance by the GP's Primary Health Organisation) until one of the two things above can take place.

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

Disposal

Health agencies need to be careful to dispose of patient records securely, either by shredding or otherwise destroying records themselves or by hiring a secure destruction contractor.

Where to get additional assistance

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

For more detailed information, a copy of the Health Information Privacy Code (with explanatory commentary) is available from the Office of the Privacy Commissioner's website at www.privacy.org.nz/.

For enquiries, the Office of the Privacy Commissioner has an 0800 number, 0800 803 909 and an AskUs knowledge base of frequently asked questions – https://www.privacy.org.nz/tools/knowledge-base/.