

HEALTH INFORMATION PRIVACY CODE FACT SHEET 1

Overview

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.

Key concepts in the Code

The two key concepts are:

- **Purpose:** Agencies must know *why* they are collecting health information and collect only the information they need. Once health information has been collected from a patient for a particular purpose, it can be used or disclosed for that purpose without additional consent.
- **Openness:** Agencies need to let patients know how their information is going to be used and disclosed so the patients can make decisions about whether to provide it.

“Ownership” of health information is a red herring

It's common for people to wonder who owns their health information. However, ownership isn't necessarily the best way to think about health information.

It is more accurate to say that:

- People have **rights** over health information about themselves. Rule 6 gives individuals the right to access information about themselves and rule 7

gives them the right to seek correction of that information if they think it is inaccurate or misleading.

- Health agencies have **obligations** over the health information they hold. These obligations are set out in the 13 rules of the Code and are briefly summarised below and in the other fact sheets in this series.

Patient expectations about health information

The Code recognises that people expect their health information:

- to be kept **confidential**, because it was probably collected in a situation of confidence and trust
- to be treated as **sensitive**, because it may include details about body, lifestyle, emotions and behaviour
- may have **ongoing use** if a piece of medical information becomes clinically relevant even a long time after it was initially collected
- will be **used for the purposes** for which it was originally collected, and they will be **told about** those purposes.

The Code's 13 health information privacy rules

The Code applies rules to agencies in the health sector. When it comes to health information, the 13 *rules* of the code substitute for the 13 *principles* of the Privacy Act.

From the point of view of a health agency, the rules in the Code can be summarised:

1. Only collect health information if you really need it.
2. Get it straight from the people concerned where possible.
3. Tell them what you're going to do with it.
4. Be considerate when you're getting it.
5. Take care of it once you've got it.
6. People can see their health information if they want to.
7. They can correct it if it's wrong.
8. Make sure health information is correct before you use it.
9. Get rid of it when you're done with it.
10. Use it for the purpose you got it.
11. Only disclose it if you have a good reason.

12. Make sure that health information sent overseas is adequately protected.
13. Only assign unique identifiers where permitted.

The first 12 rules form a kind of 'life-cycle' for health information.

Agencies must first **decide what information they need**, and where and how they are going to get it. They then need to ensure they hold the information with **appropriate protections** and that they comply with any **access or correction requests** they receive. Finally, **use and disclosure** need to be done with care and kept in line with the purposes for which the information was collected.

There are also a number of exceptions to the general rules listed above. For instance:

- Doctors can collect information about a patient's family member's health when **preparing a family or genetic history** (which could otherwise breach rule 2 since it's not being collected from the family member directly).
- Hospitals can disclose basic information to enquirers about **a hospital patient's presence, condition and progress** (as long as the patient or their representative hasn't directly vetoed that disclosure).
- Doctors can disclose information about a patient to **caregivers or close relatives** in line with recognised professional practice (again, as long as the patient hasn't vetoed that disclosure).
- Health agencies can disclose information where necessary to deal with a serious **threat to anyone's health or safety**.

The other fact sheets in this series have more detailed information on the rules.

How the rules are enforced

The first stop for a complaint will always be the agency itself. Under the Code, agencies have to have privacy officers and complaint handling procedures.

These rules are all enforceable by complaining to the Office of the Privacy Commissioner's office, and then, if necessary, to the Human Rights Review Tribunal. **There can be financial consequences for agencies that breach the rules**, so compliance is important.

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/>.