

Privacy Act 1993 and the Health Information Privacy Code 1994.

Ngati Kahu Hauora undertakes to respect and protect the privacy of all our patients and staff in accordance with the Privacy Act 1993 and the Health Information Privacy Code 1994.

To meet this commitment, we will take all practicable steps to:

- Ensure patients personal privacy should be respected at all times
- Protect our patients personal and health information including details of their medical history and disabilities
- Be proactive in anticipating privacy issues
- Comply with legislation

The Health Information Privacy Code 1994

The Health Information Privacy Code 1994 regulates how health agencies (such as doctors, nurses, pharmacists, health insurers, Primary Health Organisations and District Health Boards) collect, hold, use and disclose health information about identifiable individuals.

Key concepts in the code

The two key concepts in the code 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.

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 twelve health information privacy rules

The code applies rules to agencies in the health sector. When it comes to health information, the 12 *rules* of the code substitute for the 12 *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. Only assign unique identifiers where permitted.

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 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.