# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workbook layout</td>
<td>3</td>
</tr>
<tr>
<td>Introduction</td>
<td>4</td>
</tr>
<tr>
<td>What is privacy?</td>
<td>6</td>
</tr>
<tr>
<td>The Office of the Privacy Commissioner</td>
<td>6</td>
</tr>
<tr>
<td>The Privacy Act 1993</td>
<td>9</td>
</tr>
<tr>
<td>The aim of the Privacy Act</td>
<td>9</td>
</tr>
<tr>
<td>The privacy principles</td>
<td>9</td>
</tr>
<tr>
<td>Health Information Privacy Code (HIPC)</td>
<td>11</td>
</tr>
<tr>
<td>Providers under the Code</td>
<td>14</td>
</tr>
<tr>
<td>Definition of ‘personal information’</td>
<td>15</td>
</tr>
<tr>
<td>The role of privacy officers</td>
<td>17</td>
</tr>
<tr>
<td>Mental health information</td>
<td>19</td>
</tr>
<tr>
<td>Rule 1 - purpose for collection</td>
<td>22</td>
</tr>
<tr>
<td>Setting your purpose and being open about it</td>
<td>22</td>
</tr>
<tr>
<td>Rule 2 - source of information</td>
<td>27</td>
</tr>
<tr>
<td>Some exceptions to rule 2</td>
<td>29</td>
</tr>
<tr>
<td>Rule 3 - what to tell an individual</td>
<td>33</td>
</tr>
<tr>
<td>Some exceptions to rule 3</td>
<td>40</td>
</tr>
<tr>
<td>Rule 4 - manner of collection</td>
<td>42</td>
</tr>
<tr>
<td>Collection rules summary</td>
<td>47</td>
</tr>
<tr>
<td>Rule 5 - storage and security</td>
<td>49</td>
</tr>
<tr>
<td>Physical and operational security</td>
<td>50</td>
</tr>
<tr>
<td>Transmission and disposal (or destruction)</td>
<td>52</td>
</tr>
<tr>
<td>Data breach</td>
<td>57</td>
</tr>
<tr>
<td>Dealing with a data breach</td>
<td>58</td>
</tr>
<tr>
<td>Containment / assessment and evaluation of risks</td>
<td>59</td>
</tr>
<tr>
<td>Notification and prevention</td>
<td>60</td>
</tr>
<tr>
<td>Rule 6 - access</td>
<td>64</td>
</tr>
<tr>
<td>----------------</td>
<td>----</td>
</tr>
<tr>
<td>Requests</td>
<td>65</td>
</tr>
<tr>
<td>Timeframes for response</td>
<td>68</td>
</tr>
<tr>
<td>Charging</td>
<td>68</td>
</tr>
<tr>
<td>Some withholding grounds</td>
<td>69</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rule 7 - correction</th>
<th>80</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Rule 8 - accuracy</th>
<th>84</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Rule 9 - retention</th>
<th>87</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Rule 10 - use</th>
<th>90</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Rule 11 - disclosure</th>
<th>92</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Rule 12 - unique identifiers</th>
<th>112</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Internal complaints process</th>
<th>114</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Interference</th>
<th>116</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Complaint intake process</th>
<th>122</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Complaints process</th>
<th>124</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Glossary</th>
<th>128</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Additional resources</th>
<th>130</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Appendix</th>
<th>131</th>
</tr>
</thead>
</table>

| The HIPC rules: quick reference guide | 131 |
This workbook contains several types of study material, as indicated by the following icons.

**Key point**
This may include definitions, interesting points or where to find extra information. It will also show the steps that MUST be taken. They are very important for your learning, and to follow the law.

**Key question**
This introduces questions to reflect on or discuss through each section.

**Insights for agencies**
This shows some key information and advice for agencies from experts and other agencies.

**Self-check activity**
This activity provides an opportunity to reflect on your own organisation and to practise and evaluate your own understanding of the material.

**Group activity**
This activity provides an opportunity for you to interact within a group. It could be a discussion in pairs or a brainstorm or activity in a larger group.

**Case note**
This is a description of a real life example, to show how the theory being taught may be applied in practice.
Introduction

The Health Information Privacy Code 1994 (HIPC or ‘the Code’) regulates the way that health agencies deal with health information (sometimes referred to as ‘health data’). A good rule of thumb to keep in mind when considering how the HIPC applies is to ‘put yourself in the shoes’ of the individual concerned and to think about how you would like your own information to be treated.

This material aims to introduce you to key concepts and definitions relating to the rules of the HIPC and how they may be applied in practice. This workbook will then focus on the 12 health information privacy rules contained in the Code and will consider how they apply in practice. The workbook will also discuss the requirement for agencies to have an internal process for responding to complaints about breaches of the HIPC. Finally, we will look briefly at the consequences if there is a breach of the Privacy Act, including the test for an ‘interference with privacy’, the complaints process followed by the Office of the Privacy Commissioner (OPC) and possible court proceedings.

Because every case is different, this material is not designed to provide an exact answer about what view the OPC will form on a particular set of facts. However, this workbook will help you to recognise what parts of the Code will be relevant in the circumstances.

Figure 1 - The data an agency keeps includes information about people
1. Follow the directions of your facilitator to introduce yourself by giving:
   - your name
   - your agency / role / position
   - what kind of privacy issues arise in your work
   - what you are hoping to get out of the session

2. Use this space to make notes of people’s names, and any privacy issues you had not previously thought of.
What is privacy?

Key question

What is privacy?

Privacy is not secrecy or confidentiality
Privacy is wider than security
Privacy is about control

In the context of the Code, privacy is not about 'ownership', but about control. Individuals should be able to control the flow of information about themselves. Individuals should be able to know who is collecting, holding and disclosing information about them, and for what purpose. They should also be able to access and correct that information.

Privacy is also about defining the extent to which we as individuals interact with society and the point at which society has no need to know about who we are and what we do.

The Privacy Act and the HIPC contain these notions of control. The Act and the Code provide individuals with the ability to know what is happening to their information and retain a measure of autonomy in that process.

The Office of the Privacy Commissioner

Key question

What is the OPC?

The OPC is an Independent Crown Entity which means that it is not a direct part of the government. This is important because the OPC enforces the Privacy Act and investigates public sector agencies and so it needs to be independent of them.
Figure 2 - The OPC assists with investigation, conciliation and analysis

As well as the Commissioner, there are around 30 employees at the OPC which cover the roles of policy, investigations, communications and administration.

**Key point**

You may often hear the Office of The Privacy Commissioner called the ‘OPC’ or the ‘Office’.
The Office has a wide range of functions, which include:

- **advice** - sharing information and advice with agencies and individuals
- **education and awareness** - running education seminars and workshops to promote awareness of the Act and how it operates
- **monitoring technological change** - monitoring and examining the impact that technology has upon privacy
- **monitoring data** - monitoring data-matching programmes between government departments
- **examining new legislation** - keeping up with the possible impact of new laws on individual privacy
- **making laws** - developing Codes of Practice for specific industries or sectors; checking draft legislation
- **investigations** - investigating complaints about breaches of privacy

![Figure 3 - What the OPC does](image)
The Privacy Act 1993

To understand the HIPC, you must also understand the Privacy Act. The Privacy Act is the piece of legislation (law) that deals with the privacy of personal information or data. The Privacy Act is not about physical intrusions on privacy (such as someone looking in your bedroom window).

The aim of the Privacy Act

The aim of the Privacy Act is to give individuals more control over their personal information. The Act requires that when agencies are going to be collecting, holding and using personal information, that they are clear about what they are doing and why. The Act also provides individuals with the right to access and correct that information.

The focus of the Act is on purpose not consent. So, when an agency collects personal information, if it intends to disclose (tell another personal or agency) the information, for whatever reason, it needs to make the individual aware of this.

Once it has done so, and the individual then chooses to provide the information, the agency is free to disclose the information if it wants to; it doesn’t require any further authorisation from the individual concerned.

The privacy principles

There are 12 information privacy principles that deal with the collection, storage, use and disclosure of personal information, and give people the right to access and correct their information.

The Commissioner can issue industry-specific Codes of Practice, which modify the 12 information privacy principles to deal with specific types of information in a way that fits well with the particular industry. The main Codes are:

- Health Information Privacy Code (HIPC)
- Telecommunications Privacy Code
- Credit Reporting Privacy Code
Key point

There are twelve principles to do with how private information can be collected, stored, used and disclosed. If these are not followed, a complaint may be made to the Privacy Commissioner. These are reflected in the 12 rules of the Health Information Privacy Code (HIPC).

Insights for agencies

The term ‘data’ is not helpful and can invite complacency because it makes people forget that it is information about people.
The Health Information Privacy Code (HIPC) is a Code of practice issued by the Privacy Commissioner. The Code modifies the 12 privacy principles in the Act into 12 rules which are designed to deal more specifically with privacy issues arising in the health context. These rules cover:

- collection
- disclosure
- access and correction
- storage, accuracy, retention, use and unique identifiers

The rules are enforceable by complaining to the Privacy Commissioner.

The HIPC also introduces the requirement for health agencies to follow a specific process when responding to complaints from individuals about potential breaches of the Code.

**Key point**

The Health Information Privacy Code (HIPC):

- is a Code of practice issued by the Privacy Commissioner
- focuses on **purpose** (not consent)
- modifies the 12 information privacy principles of the Privacy Act into 12 rules
1. Only collect personal information you really need.
2. Get it directly from the person where possible.
3. Be open with people about what's going to be done with it.
4. Be fair about how you get it.
5. Keep it secure.
6. Let the person see it if they want to.
7. Fix it if the person thinks it's wrong.
8. Take care that it's accurate before using it.
9. Dispose of it when it's no longer needed.
10. Use it only for the purpose for which you got it.
11. Only disclose it if you have good reason to do so.
12. Only use ‘unique identifiers’ where this is clearly allowed.

Figure 4 - The principles of the Privacy Act
### A general summary of the rules

The 12 rules have, in very general terms, the following effect:

<table>
<thead>
<tr>
<th>Rule</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule 1 - purpose for collection</td>
<td>Only collect information when you need it for a lawful purpose connected with your agency.</td>
</tr>
<tr>
<td>Rule 2 - source of information</td>
<td>Obtain the information directly from the person concerned if possible.</td>
</tr>
<tr>
<td>Rule 3 - what to tell an individual</td>
<td>Tell the person what you are doing.</td>
</tr>
<tr>
<td>Rule 4 - manner of collection</td>
<td>Do not use unfair or unreasonably intrusive means of collecting the information.</td>
</tr>
<tr>
<td>Rule 5 - storage and security</td>
<td>Take care of the information once you have obtained it.</td>
</tr>
<tr>
<td>Rule 6 - access</td>
<td>The person can ask to see the information.</td>
</tr>
<tr>
<td>Rule 7 - correction</td>
<td>The person can ask you to correct the information.</td>
</tr>
<tr>
<td>Rule 8 - accuracy</td>
<td>Make sure that the information is accurate before you use (process) it.</td>
</tr>
<tr>
<td>Rule 9 - retention</td>
<td>Dispose of the information once you have finished with it.</td>
</tr>
<tr>
<td>Rule 10 - use</td>
<td>Only use the information for the purpose for which it was obtained.</td>
</tr>
<tr>
<td>Rule 11 - disclosure</td>
<td>Only disclose the information if this was the reason for which you obtained it.</td>
</tr>
<tr>
<td>Rule 12 - unique identifiers</td>
<td>Only use unique identifiers in place of person's name where necessary.</td>
</tr>
</tbody>
</table>

Table 1 - A general summary of the HIPC rules
The information life cycle

As you will see, a piece of information has a life cycle involving:

- what you need to think about before you collect personal information
- what you need to consider once you have obtained the information
- what you need to take into account when you are using or disposing of the information

For example, if you are going to collect information, the Act tells you that the first thing you must do is decide why you need the information (rule 1). If you know why you are collecting the information, you can then tell the person concerned why you need it (rule 3). You are then able to use (or disclose) the information for that purpose (rules 10 and 11).

Providers under the Code

There is broad coverage of what constitutes an agency under the Code. All agencies that provide a health or disability service are covered - from large hospitals to sole practitioners. Some examples include:

- rest homes, doctors, nurses, dentists, pharmacies, psychologists
- purchasers for purposes of the Health and Disability Services Act 1993
- ACC and other health insurers
- educational institutions which train health professionals
- statutory bodies responsible for registration and discipline of health professionals
- agencies such as the Ministry of Health and the Health Research Council

These are examples only and there are more agencies which may come under the Code.

Figure 5 - Health providers have a responsibility to collect information for purpose
Definition of ‘personal information’

The Code applies to personal information about an identifiable individual. The Privacy Act defines the word ‘individual’ as a natural person (as opposed to a body corporate or company) other than a deceased natural person.

Note that the HIPC can also apply with respect to health information about deceased persons in limited circumstances - see rule 11 of the HIPC and section 22F of the Health Act 1956.

The word ‘information’ is not defined in the Code, but the High Court has said that it is not confined to the written word, but embraces any knowledge however gained or held, and, in some circumstances, can extend to information held in the mind of an individual. As such, information about an individual could include written notes, emails, audio and CCTV recordings, photos or a summary of comments made about the individual during a recent discussion.

Figure 6 - Personal Information is about an identifiable individual
Health information about an identifiable individual

The Code applies to health information about an ‘identifiable individual’, including:

- medical and treatment history
- disabilities and accidents
- contact with any health / disability provider
- information about donations of organs, blood, etc.
- incidental information obtained while providing services such as billing, subsidy entitlements, etc.

Information without identifiers

If an individual is not identifiable, then the Code will not apply. However, care needs to be taken when ‘anonymising’ information, as simply removing someone’s name may not mean that the information is no longer identifiable. As an example, in some circumstances a description of a disease or set of events will be enough for someone to identify who is being discussed, even if their name is not used.

Limits

Section 7 overrides

If another law authorises or requires collection, use or disclosure, or limits an individual’s right of access, then that law will override the Code.

The statutory basis for this is section 7 of the Privacy Act. This is also known as a ‘section 7 override’:

- Some legislation may authorise or provide an agency with discretion to carry out an action. If the agency uses its discretion, the Code won’t apply.
- Other legislation may require an agency to perform an action. In this instance, the agency must comply and the Code will not apply.
Household affairs

The rules generally do not apply to information held or used in connection with your personal, family or household affairs. In other words, if you acquire a piece of information through work, it’s treated differently from how it would be if you obtained that piece of information from your friends and family.

However, if you collect, use or disclose health information in a way which would be highly offensive to a reasonable person, then the rules may apply even if you collected, used, or disclosed that information in a personal capacity. More information on this is available in section 56 of the Privacy Act.

Agencies are responsible for employees’ actions

An agency has a responsibility to ensure that its employees adhere to the Act. Therefore, the agency is deemed to be responsible for any actions an employee takes in the course of their employment, or if an employee uses personal information they obtained in the course of their employment. However, the agency will have a defence if it can show that it did everything reasonable to prevent its employee from acting in this way. In such cases, the individual may be held directly liable.

Key point

More information on the defence that the agency did everything possible to stop a breach action, and is therefore not liable, can be found in section 126 of the Privacy Act.

The role of privacy officers

The Privacy Act, section 23 states that every agency must appoint a privacy officer. The privacy officer is responsible for:

• ensuring that the agency complies with the Act
• dealing with requests made to the agency for access to, or correction of, personal information
• working with the Privacy Commissioner’s Office when it investigates complaints

To do this, the privacy officer needs to be familiar with the Privacy Act and the agency’s obligations under the Act, as they apply to their agency.
Self-check activity

Answer the questions below about the privacy officer at your agency. If you are your agency’s privacy officer, reflect on the questions and answer them according to your own role.

1. What is the privacy officer’s name?

2. How are the privacy officer’s contact details communicated:
   a) to agency staff?
   
   
   
   
   b) to the public?
   
   
   

3. What do I know about the responsibilities of the privacy officer’s role?

   
   
   

4. What tasks has the privacy officer completed within their role?

   
   
   

5. Has the privacy officer assisted with an OPC complaint?

   
   
   

---

HEALTH 101: AN INTRODUCTION TO THE HIPC
Mental health information

Mental health is often regarded as more sensitive than ordinary health information due to media interest, public concern and the perceived stigma associated with mental illness.

There are potentially serious consequences for:

- the individual if information is inaccurate, misused or disclosed without their authority; and
- family / friends / employers, in the case of failure to disclose

Sharing of information in a mental health services environment requires the balancing of interests of four key groups:

1. **The individual or service user to whom the information relates**
   
   The individual would expect that their information is kept confidential and wants to retain some control of the information based on their right to privacy. There is also a risk that, in the hands of others, information may be used against them.

2. **Agencies providing clinical care or other services**
   
   The health provider / clinician needs to be able to share health information sufficiently to provide optimum care and ensure the safety of others while focusing on treating the individual.

3. **Family / whānau of those involved in support**
   
   Under the [Mental Health Act](https://www.mayoclinic.org/symptoms/mental-health/ds00819) agencies also have an obligation to include families / whānau and significant others in order to support the treatment process. They have an interest in being kept informed about what is happening to their family member.

4. **The wider community (including media)**
   
   Sometimes the wider community has an interest, including media providers. If the service user was discharged and integrated into the community, then the public may wish to know as they have an expectation that they should be safe in their own environment, and that any risks to them are appropriately recognised and managed.

   It is fair to say that tension between these interests does occur and, more often than not, these are the situations where decisions about sharing health information become difficult.
The Code does not differentiate between ‘health information’ and ‘mental health information’.

However, there are some exceptions in the rules that are specific to mental health circumstances as follows:

- Collection from third parties is allowed if an individual is unable to provide information.
- Disclosure of mental health information in particular circumstances; and
- The ability to refuse access if disclosure would endanger safety or prejudice mental health.
### Self-check activity

1. Reflect on how sensitive information is handled at your agency and complete Table 2.
2. Talk to your supervisor or more experienced workmate where applicable.

<table>
<thead>
<tr>
<th>Mental health information collection</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Question</strong></td>
</tr>
<tr>
<td>What groups may have an interest in the mental health information of our patients or clients?</td>
</tr>
<tr>
<td>When might the person be unable to provide information themselves?</td>
</tr>
<tr>
<td>When might direct collection compromise the patient’s treatment?</td>
</tr>
</tbody>
</table>

Table 2 - Mental health information collection reflection
Rule 1 - purpose for collection

Key point

Rule 1

Health information must only be collected when:

- the collection is for a lawful purpose
- the purpose is connected with the functions of the agency, and
- it is necessary to collect the information for that purpose

Setting your purpose and being open about it

Rules 1-4 of the Code concern the collection of personal health information.

The Code states that agencies have to do the following two things:

1. **Set a purpose** - develop policies for information.
2. **Be open about it** - tell individuals about those policies when they collect this information.

Agencies are not allowed to collect personal information from people unless:

1. information is collected for a lawful purpose connected with a function or activity of the agency, and
2. collection is necessary for that purpose

Rule 1 is about what information an agency is allowed to collect. It is designed to stop agencies from collecting information that they do not need.
Key point

Rule 1 is written to stop excessive collection of information. It is designed to encourage agencies to set a purpose for collection and be open about it.

Understand the collection process

It is very important to understand the collection process, because it relates directly to the guidelines around how the information can be used and disclosed. The first step for an agency is to set its purpose in compliance with rule 1. Once an agency knows exactly what its purpose is for collecting personal information, this will enable the agency to properly communicate this purpose to individuals when it collects their information (rule 3) and then later uses or discloses this information (rules 10 and 11) in compliance with the Code.

Agencies must set their own purpose:

To comply with rule 1, agencies must set their own purposes with regard to the information they collect. In doing so, the agency must ask itself the following question:

Do I have a lawful purpose for collecting the information?

To figure this out, you must then ask:

- **What** information do I need to collect?
- **Why** do I need this information?
- Is there a law about **how** to do this?
- Is the **purpose** connected with a function or activity of the agency?
- Is the collection of this information **necessary** to achieve that purpose?

Many agencies fail on the last point. By not asking if it is necessary to collect the information, you may breach the Code.
Rules 1-4 only apply when an agency **collects** personal information. While the term ‘collect’ has been given a broad meaning (‘gathering together, the seeking of or acquisition of personal information’), if an agency receives **unsolicited** information, then rules 1-4 will not apply.

As an example, if an agency received a tip-off that one of its employees was lying about being on sick leave when they were actually taking a holiday, along with photos of the employee from Facebook as proof, this would not raise issues under rules 1-4.

However, don’t forget that, no matter how the agency obtained the personal information, once it holds the information, the other rules (5-12) will still apply.

**Key question**

What if we receive information we didn’t ask for?

**Insights for agencies**

Develop simple and easy to understand policies and guidelines about privacy.
1. Follow the directions of your facilitator to form groups.
2. Complete the task as directed by your facilitator.
3. Use the space provided to write any notes or questions.
A man applied for trauma insurance providing extensive medical information and authorising the insurance company to collect health information relating to the application and any previous claims. The insurance company contacted the man’s GP and obtained the man's full medical history for the preceding five years.

When we investigated the complaint the insurance company advised it had identified three issues in the application which it had wanted further information about.

We formed the view that the company should only have requested information relating to the three issues and that, as a result, it had breached rule 1 of the HIPC by collecting five years of the man's full medical history.

The insurance company accepted our view and amended its process so that it only asked for information relating to specific conditions identified in applications. It also reached a confidential settlement with the complainant.
Rule 2 - source of information

Rule 2 relates to the sources from which an agency can collect personal information.

When collecting information or planning to collect information, ask yourself the following:

1. If you want to collect information about an individual, who is the best person to collect that information from?

2. Under what circumstances might you need to collect it from someone else?

Generally, health information should only be collected from the individual concerned. This ensures that the person knows that information is being collected from them. They also know what information is being collected, and have the opportunity to exert some control over what is collected.

Key point

Rule 2

Health information must usually be collected from the person who the information relates to. But the Code does allow you to collect information from other people in limited cases, for instance, when:

- the person concerned authorises collection from someone else
- obtaining it from the person concerned would undermine the purpose of the collection
- this is necessary in order for a public sector body to uphold or enforce the law, or
- this is necessary for the purposes of court or tribunal proceedings
Group activity

1. Follow the directions of your facilitator to form pairs or small groups.
2. Discuss examples of when an agency might want to collect information from people other than the individual concerned.
3. Use the space provided to write any notes or questions.

____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
Key point

When sourcing personal information for your agency’s purpose, ensure that you only collect information from the individual concerned, unless an exception applies.

The test for believing that an exception applies is reasonable grounds (what is reasonable will depend on the circumstances).

It is up to the agency to establish that reasonable grounds existed (this is covered in section 87 of the Privacy Act), so if you do collect information from anyone other than the individual concerned it is best practice to document why you considered that an exception applied in that case.

Some exceptions to rule 2

In some cases an exception may be made to rule 2; these instances are detailed below.

Authorisation given

This means the person specifically allows the information to be collected from someone else. This exception is read in conjunction with rule 3(1), which provides, in part, that the individual should understand:

- what is to be collected
- from whom it is to be collected (collection may be restricted to one particular person)
- the purposes for obtaining the information, and
- who will receive it

The individual should clearly understand who they are allowing to give what information. Safeguard yourself by requiring the authorisation to be explicit, clearly defined and, if possible, in writing, so that if any problems arise at a later date then a written record of what was authorised exists.
Key point

When collection is authorised from another person, make sure you keep yourself and your agency safe by getting this clearly in writing and making sure the client or patient understands fully what they are authorising.

Prejudice the purpose of collection

For example, a patient may be displaying behaviour which indicates they are unwell, but insists that there is no problem, or may modify their behaviour. Without information from another source that the patient is unaware of, treatment may not be as effective.

Another instance where this exception could apply would be where collecting information from a person in an acute state with a mental illness might compromise their treatment. In such cases the information might have to be collected from another person who is in a better position to supply it, in order to ensure proper treatment is provided. Accuracy should be verified with the individual where practicable.

Compliance is not reasonably practicable in the circumstances

An agency would rely on this exception where the patient may not be able to provide the information and without accurate information from another source their health may be compromised. For example, the patient may be unconscious or incapable. Another example would be where the individual has a significant intellectual disability or an acute mental illness and is unable to understand what is being asked.

Compliance would prejudice the safety of another person

It may be safer for a staff member to ask a third party for information, as the patient may be violent.

Individual not identified

If information is to be used for statistical or research purposes and will not be published in a form that would identify the person, or if the information has the identifier removed and the client or patient could not be identified by other data, then this may be used without obtaining their permission.

Where the information is sourced from a publicly available publication

You do not need to obtain permission from an individual to collect information about them from a publicly available source, such as a newspaper or the internet. For more information about what is meant by 'publicly available' see section 2 of the Privacy Act.
1. Follow the directions of your facilitator to form pairs or small groups.
2. Complete the task as directed by your facilitator to complete Table 3.
3. Use the space provided to write any notes or questions.

<table>
<thead>
<tr>
<th>Exception</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorisation given</td>
<td></td>
</tr>
<tr>
<td>Prejudice the purpose of collection</td>
<td></td>
</tr>
<tr>
<td>Not reasonably practicable</td>
<td></td>
</tr>
<tr>
<td>Prejudice the safety of any individual</td>
<td></td>
</tr>
<tr>
<td>Individual not identified</td>
<td></td>
</tr>
<tr>
<td>Information publicly available</td>
<td></td>
</tr>
</tbody>
</table>

Table 3 - Exceptions to rule 2
Key point

When sourcing health information for your agency’s purpose, ensure that you only collect information from the individual concerned, unless an exception applies.

The test for believing that an exception applies is reasonable grounds. What is considered ‘reasonable’ will depend on the circumstances.

- It is up to the agency to establish whether reasonable grounds exist (section 87 of the Privacy Act), so it is best to document why you believe the exception applies.

Example: case note 7454

The complainant was admitted to a mental health unit for assessment after his wife reported that she had concerns about his mental state.

Mental health staff carried out an initial assessment. As part of that assessment they approached the complainant directly. However, he refused to talk to them, so the staff approached his doctor, former employer and his minister. The complainant alleged that this amounted to a breach of rule 2.

The Commissioner was of the view that, as the complainant was unwilling to supply the information and as he was unable to provide the information sought, it was not reasonably practicable to collect the information directly from the complainant.

Key point

If information is collected from someone other than the person themselves, it is prudent to note it on the file and, when, or if appropriate, check the accuracy with the individual in order to ensure compliance with rules 7 and 8, which relate to accuracy.
Rule 3 - what to tell an individual

Key point

Rule 3

When an agency directly collects health information, it has to take reasonable steps to make sure that person concerned knows things like:

- why it is being collected
- who will see the information
- whether the person is required to give the information or whether it is voluntary
- what will happen if the information isn’t provided

Again, there are sometimes good reasons for not letting a person know. For example, it could undermine the purpose of the collection, or it is just not possible to tell the person.

Rule 3 is about ensuring awareness of what is being collected. An agency should be open about what it is collecting and why.

Take reasonable steps to ensure that they are made aware of what information is being collected, and why the information is being collected. This helps prevent misunderstandings which can be critical later when using or disclosing information.

Tell people why you are collecting their information and what you are going to do with it. A good example of this is provided in Figure 8.
### Ora Pai Ake Patient Information Form

The information from you in this form is required for the purpose of providing and administering health care. Should you not wish to provide any information requested please contact a member of staff who will explain the consequences of not supplying it.

#### Your Details

<table>
<thead>
<tr>
<th>Title:</th>
<th>Family name</th>
<th>First name(s):</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Any previous names:</th>
<th>Preferred name:</th>
<th>Address:</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Do you speak English?</th>
<th>Place of birth:</th>
<th>Date of birth:</th>
</tr>
</thead>
<tbody>
<tr>
<td>□ Yes □ No</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phone:</th>
<th>Mobile:</th>
<th>Sex: □ M □ F</th>
</tr>
</thead>
</table>

#### Ethnicity

- NZ Māori
- NZ Pākeha
- Indian
- Chinese
- Tongan
- Cook Islander
- Fijian
- Niuean
- Samoan
- Tokelauan
- European
- Pacific
- Islander
- Asian
- South East
- Not Known
- Other (specify)

#### Services

- **Maori Health Unit**
  - Would you like a visit from a member of the Māori Health Unit?
  - □ Yes □ No
  - This service is voluntary and is available to anyone.

- **Chaplaincy / Church Minister**
  - A Chaplaincy Service is available. Would you like to be visited?
  - □ Yes □ No
  - If yes, which denomination / Church do you attend?
  - If you tick yes and provide your details, the Chaplaincy service will be made available to you.

#### Residency

- Are you a permanent resident of NZ?
  - □ Yes □ No

- If No, have you lived in New Zealand for more than two years?
  - □ Yes □ No

#### Occupation

- If you are retired, please state Retired and previous occupation.

#### Emergency Contact Person

<table>
<thead>
<tr>
<th>Name:</th>
<th>Relationship:</th>
<th>Contact details:</th>
</tr>
</thead>
</table>

#### Family Doctor

<table>
<thead>
<tr>
<th>Family doctor:</th>
<th>Address:</th>
</tr>
</thead>
</table>

---

**Note:**
- The information provided is confidential.
- It is used for the purpose of providing and administering health care.
- If you have any concerns, please contact a member of staff.
- This form is compliant with privacy laws.

---

**Privacy Commissioner**
- Te Mana Matapono Matatapu

---

**HEALTH 101: AN INTRODUCTION TO THE HIPC**
### Who will see this information?

Your health information will only be passed on to:

- Staff involved in providing and administering health care treatment to you
- Outside agencies which assist us in providing you care, e.g. testing labs
- Staff and Funding Purchasers (this information is usually non-identifying)
- The Ministry of Health for health and research and statistical purposes

Your information will not be passed on to any other agency unless it is authorised or required by law.

### Why is this information needed?

#### Your Details

It is very important that we are able to identify you from your records so that we do not confuse you with anyone else. This requires knowing any past names you might have been known by, including your maiden name.

<table>
<thead>
<tr>
<th>Ethnicity</th>
<th>Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Ministry of Health requires this information, for statistical purposes. It also assists the Government with its obligations under the Treaty of Waitangi.</td>
<td>This shows which services you would like to be available to you. These are completely voluntary and available to anyone. If you tick yes and provide your details, the Chaplaincy service will be made available to you.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Residency</th>
<th>Occupation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your entitlement to health care services may depend on your residency status. If you have lived in New Zealand for under two years you will be required to supply further information.</td>
<td>Your occupation may affect your health. Supplying this information ensures you receive the appropriate care.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Emergency Contact Person</th>
</tr>
</thead>
<tbody>
<tr>
<td>In an emergency it is important the hospital knows who should be contacted. This person can be, for example, your next of kin, spouse, partner, close friend or neighbour.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Family Doctor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your GP may be required to supply details from your file. Your health information will also be made available to your GP on discharge.</td>
</tr>
</tbody>
</table>

**Figure 8** - Example health admission form
Rule 3 statement

Key question

When you collect information directly from the individual, what should you tell them at the time that you collect the information?

Take reasonable steps to ensure that people are aware of what information you are collecting and why you are collecting it. This will help to prevent any misunderstandings, and can be critical later when you use or disclose the information. If you know that you are going to disclose the information because that is your purpose, then say so.

This information forms what the OPC calls a rule 3 statement. The information can be conveyed in a number of ways, including:

- telling the person in a language that they understand
- putting notices or signs on display
- providing letters and brochures, or including statements on the form to be completed

It is important that the person’s attention is drawn to this information. If the information is provided on a form to be completed by the person, they should be able to either take a copy with them or access the information elsewhere, e.g., on your agency’s webpage.

Key point

If practicable, this information must be provided before collection.

When you are collecting information from people, be open about it. Tell them why.

It may be useful to think about what you would like to know before you hand over your personal information – working on a ‘no surprises’ basis is best!
You need to tell people all of the following:

**The fact that information is being collected**

It is not always obvious that information is being collected or that it is being collected in a particular way, so don’t assume people know. If an audio or video recording is being made, is the recording equipment in plain view, and has it been pointed out to them?

**The purpose for collection**

Give a good indication of why information is being collected and what it will be used for. If you only tell the person a very small part of what the information will actually be used for, this could cause problems for your agency when you try to use it later on. However, if the purposes that you give are too broad, then informing the person will become pointless.

Always be aware that the less obvious purposes are the ones that could cause people distress. So make sure that you tell people about these ones particularly. The following case note is a medical example that illustrates this point well.

**Who will see the information**

Individuals should be told of the agency’s practices and anticipated disclosures. You don’t need to tell them about absolutely every possible disclosure - just give a general indication of who is likely to see the information and the reasons they will need to see it. In the following case note, clinical staff are obvious recipients, but researchers, students and hospital chaplains would not be.

Equally, members of a ‘care team’ may not be obvious, depending on the circumstances. In most situations the number of people who will have access to patient information is high, which makes this requirement important.
Case note: use of religious information

It is common practice for hospitals to ask for the religion of patients. It is not always apparent why this information is required. Often there is no other reason for asking except to inform the hospital chaplain.

However, when individuals are not told there can be unanticipated adverse consequences.

In one case investigated by the Office a 16-year-old girl was admitted for a termination. She indicated on her admission form that she was a Catholic. While she was there for the procedure, she was visited by the chaplain who observed from her notes that she had been admitted for a termination.

The chaplain relayed this information to her parents. Had the hospital phrased its request in terms of ‘If you would like to be visited by a chaplain, please indicate your religion’ this situation could have been avoided.

The contact details for the agency collecting and holding the information

Some agencies may collect information on behalf of another agency. If the information will be held by an agency other than the one collecting the information, you must let the person know who will be in charge of the information.

Whether the supply of information is voluntary or mandatory

This means whether the individual has a choice to provide the information or not.

Voluntary information is information that would be nice or useful for your agency to have, but does not affect whether or not you can provide them with service, and they are not required to give you that information under the law. Examples of this could include questions such as ‘Who referred you to our clinic?’ or research information such as permission to use your data for a study for another organisation.
Mandatory information is information that the individual must supply, because:

1. if they don’t supply the information then you cannot enrol them or provide them with a service, e.g., if an individual does not provide relevant health or injury history to a massage therapist, they may refuse to treat them on the grounds of safety

OR

2. they are required to give the information by law, e.g., departure cards are required to be filled out under immigration law

Where your agency is relying on another specific piece of law to collect personal information, you need to let people know:

1. what the piece of law is, and
2. whether they have a choice to tell you the information or not

Some laws will allow agencies to collect certain personal information but do not oblige the individual to provide the information if they don’t want to. However, other laws will state that individuals are required to provide information and could, for example, be fined if they don’t.

Key point

You must tell people whether the supply of information is voluntary or mandatory:

**Voluntary** means they have a choice if they give it or not; it is useful but not essential.

**Mandatory** means they are compelled by law, or there will be consequences for them if they do not supply it.

In mandatory cases you must tell them what information is requested and the consequences if they do not supply it.

The consequences of not providing the information

Tell the person what will happen if they do not provide the information. For example, it might not be possible to process a person’s application, subsidy or benefit. In a medical context, the agency might state that a treatment might not be as effective, or could be fatal, without the correct information.
Some exceptions to rule 3

Key question

When might you not want to tell people or make them aware that you’re collecting information from them?

There are some cases where agencies will not need to provide the individual with a rule 3 statement. This is where the agency believes on reasonable grounds that an exception applies. A full list of the exceptions can be found in the Act, but some common examples are:

- **It is not reasonably practicable in the circumstances.** When an explanation would delay provision of emergency treatment, the patient is not capable of understanding an explanation at the time it is offered, or the explanation could cause a violent response.

- **It may prejudice the purpose of collection or maintenance of the law, or the safety of any person.** For example, a patient may modify their behaviour so as to prevent effective diagnosis or treatment.

This is very similar to rule 2 and there are the same types of exceptions. You must also believe on reasonable grounds that the exceptions apply. Again, as per section 87 of the Privacy Act, if your agency relies on an exception, then the burden is on you to show why the exception applied. To make this easier, the agency should document why it believes an exception applies as and when such an occasion arises.

If it is not practicable to give an explanation at the time, then as soon as possible afterwards is acceptable. It is not necessary to repeat the explanation every time information is collected from an individual for the same purpose. However, if your rule 3 information has changed, or if it has been a while since you’ve dealt with someone, you should give them a refresher.

Remember, an exception applies if:

- non-compliance is authorised by the individual concerned
- compliance is not reasonably practicable in the circumstances, or
- compliance would prejudice purposes of collection
Self-check activity

Follow the directions of your facilitator and answer the following questions:

1. Does my agency have a rule 3 statement?

   ____________________________________________________________
   ____________________________________________________________

2. Where is it located?

   ____________________________________________________________
   ____________________________________________________________
   ____________________________________________________________

3. Does it meet the criteria listed above?

   ____________________________________________________________
   ____________________________________________________________
   ____________________________________________________________

4. What exceptions have there been in my workplace?

   ____________________________________________________________
   ____________________________________________________________
   ____________________________________________________________
   ____________________________________________________________
Rule 4 - manner of collection

Key point

Rule 4
Health information must not be collected by unlawful means or by means that, in the circumstances, are unfair or unreasonably intrusive.

Personal health information must not be collected by means that are:

- unlawful
- unfair under the circumstances, or
- unreasonably intrusive

The focus of rule 4 is on the manner in which information is collected, rather than what is collected (i.e., how rather than why the information is collected). An explanation of the terms and an example of each is shown in Table 4.
<table>
<thead>
<tr>
<th>Term</th>
<th>Explanation</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unlawful</td>
<td>Would collection breach another Act?</td>
<td>For example, <a href="#">section 68 of the Mental Health (Compulsory Treatment) Act</a> restricts the use of video and audio to record patients. The recording must be done with the patient’s prior consent (or that of the patient’s representative where the patient is not capable of giving consent).</td>
</tr>
<tr>
<td>Unfair</td>
<td>Includes misleading the individual as to the purpose of collection, or threats of coercion to provide information</td>
<td>Intimidating a patient into providing information, or pretending information is ‘just between us two’.</td>
</tr>
<tr>
<td>Unreasonably intrusive</td>
<td>When considering what may be regarded as unfair or unreasonably intrusive, the agency should ask - What is it about these circumstances that justify the means used to collect the information?</td>
<td>Installing cameras in a patient examination area or a changing room.</td>
</tr>
</tbody>
</table>

Table 4 - Rule 4 breaches
Group activity

1. Follow the directions of your facilitator to form pairs or small groups.
2. Complete the task as directed by your facilitator.
3. Use the space provided to write any notes or questions.
A man became aware that his local pub had CCTV operating in the men’s restroom after seeing a still taken of him using the facilities. He complained this was an intrusive collection.

The pub manager informed us that CCTV was in operation in the pub for safety and security reasons, and confirmed the pub did have signage about the use of CCTV (although nothing explicitly said that cameras were operating in the bathroom).

We considered that general use of CCTV was reasonable as there was signage, the footage was only used for safety and security, and there was adequate protection for the information (for example, only certain staff could access it).

However, we were not satisfied there was a good reason to have a camera operating in the toilet given it was capturing highly sensitive information. On this basis we considered the pub had breached principle 4.

Based on our view the pub manager agreed to remove the camera from the toilet area.
1. Follow the directions of your facilitator to form pairs or small groups.
2. Follow the directions of your facilitator to complete Table 5.

### Collection questions

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Family information</strong></td>
<td></td>
</tr>
<tr>
<td>• Frank is a voluntary patient.</td>
<td></td>
</tr>
<tr>
<td>• Childhood could be affecting treatment.</td>
<td></td>
</tr>
<tr>
<td>• Frank does not seem to know of any incident.</td>
<td></td>
</tr>
<tr>
<td><strong>Videotaping interviews</strong></td>
<td></td>
</tr>
<tr>
<td>• Hine’s counsellor taped sessions for training courses.</td>
<td></td>
</tr>
<tr>
<td>• The counsellor said only excerpts would be used and the client would not normally be identifiable.</td>
<td></td>
</tr>
<tr>
<td>• Sensitive information was used for training.</td>
<td></td>
</tr>
<tr>
<td><strong>Reception areas</strong></td>
<td></td>
</tr>
<tr>
<td>• Phillip is a new patient.</td>
<td></td>
</tr>
<tr>
<td>• The receptionist asks him questions and enters information into computer.</td>
<td></td>
</tr>
<tr>
<td>• People can hear the discussion.</td>
<td></td>
</tr>
<tr>
<td><strong>Avoiding misunderstandings</strong></td>
<td></td>
</tr>
<tr>
<td>• Ellen’s test shows she would be a suitable donor for her sister.</td>
<td></td>
</tr>
<tr>
<td>• The specialist told the sister.</td>
<td></td>
</tr>
<tr>
<td>• Ellen had not decided whether she wanted to donate her kidney and felt pressured by her family.</td>
<td></td>
</tr>
</tbody>
</table>

Table 5 - Collection questions (rules 1-4)
Collection rules summary

Rules 1-4 mean you need to decide and communicate:

- why you are collecting - purpose
- who you collect from - source
- what you tell people when you collect their information
- how you collect information

Figure 9 - You need to tell people who will view their information
Self-check activity

Reflection

Use the space provided to create a mind map of the concepts you have learnt so far about the fair collection of personal information.
Rule 5 - storage and security

Key point

Rule 5
It is impossible to prevent all mistakes. But health agencies must ensure that they take reasonable steps to prevent the loss, misuse or disclosure of health information.

Rule 5 requires agencies to take reasonable security safeguards to protect against:

- loss
- unauthorised access, use, modification or disclosure; and
- other misuse

What is reasonable will depend on the nature of the information being held and the potential risk of harm occurring. Health information, for example, is generally considered to be inherently sensitive. However, certain types of health information, for instance information about mental health or sexual health may be considered to be especially sensitive.

Also keep in mind that the agency is responsible for the health information it holds directly, and all health information that it provides to any individual or agency acting on its behalf. So, if an agency has to give information to someone else to allow a service to be provided, it must do everything reasonable within its power to prevent the unauthorised use or disclosure of that information by the recipient.

Insights for agencies

Carry out regular audits of your agency’s IT security. Employ an IT security company to conduct penetration tests on your system to look for security flaws. Fix any weaknesses that are identified.

Have a notice counting the days since the last data breach and celebrate as an agency when the time elapsed breaks a previous record.
Physical and operational security

As an agency you are in the best position to determine the risk of harm occurring and the steps that can be taken to reduce that risk.

Below are some of the steps you should consider taking when developing a storage and security policy.

Physical security

- Implement a clear desk policy.
- Lock information away.
- Restrict unauthorised access.
- Turn computer screens and whiteboards away from public areas.
- Place computers, faxes and printers where they cannot be accessed by unauthorised personnel.

Electronic security

- Have appropriate firewalls.
- Install and update antivirus software.
- Update passwords regularly.

Operational security

- Restrict staff access to information - only allow access to information that staff need to do their jobs. This can be done physically, electronically or through the separation of files, e.g., separating personnel files into accounts, medical and performance.
- Run staff training covering:
  - the need for security for client or personnel records
  - when information may be accessed, used and disclosed
  - warnings against ‘employee browsing’ (unauthorised access of files)
Key point

Train staff and make sure they can only access what they need to do their job. Build a system that allows you to track who has accessed information.

Insights for agencies

Develop a whole-organisation approach to privacy - one that values personal information and treats it with care. For example, privacy is not just the responsibility of an agency’s legal department, because it also involves information technology, human resources and other areas.

Accountability structures need to be clear so top and senior management recognise that they are ultimately responsible for information breaches.

Where an information system is broken, shutting it down is a drastic resort but may work in some cases to prevent a wider breach.

Figure 10 - Good security practices protect your agency and individuals
Transmission and disposal (or destruction)

Transmission

Transmission of information includes the following measures.

- Implement controls on the type of information that can be sent by fax and/or e-mail.
- When using a facsimile, make a telephone call prior to transmission to ensure that the information is uplifted immediately.
- If you are relying on a contractor for information handling, have an agreement with the contractor that only duly authorised staff can access records.
- When using e-mail, use ‘nicknames’ or an address book to send information to minimise inadvertent disclosure. Encryption is something else that you may consider. You should consider turning off ‘auto-complete’ or using the ‘delay delivery’ function. You should also have clear policies around the type of information staff may or may not send by email.

Disposal

When information is no longer needed, it must be disposed of in an appropriate manner. Disposal of information could involve things like:

- using a shredder, or
- if using an outside contractor, making the secure destruction of documents a condition of the contract

It is best practice to have a policy about how and when files will be disposed of.

Figure 11 - Have a policy about how and when files will be disposed of
Case note: example of poor disposal

The Privacy Commissioner investigated a complaint where a doctor bought a practice in which there was a large quantity of patient information which required disposal. The doctor hired a digger and buried the information on the beach. After the tide came in the files were uncovered and spread along the beach.

Key point

When determining whether a security safeguard is reasonable, the Commissioner will consider:

- the sensitivity of the information
- where the information is located
- the likely harm that would occur if principle 5 was breached
- the steps and/or policies in place to guard against such a breach
- whether those steps and/or policies have been followed
- relevant training provided to staff
A man, M, was involved in Family Court proceedings with his ex-partner, X. They, and their family, had all been patients at the same medical centre.

X visited the medical centre with her new partner, N, and they requested historical information about the family and about one incident in particular. The medical centre assumed N was M and released all of the information they held about M, X and their children. X then used information about M in the Family Court proceedings.

Section 45(a) of the Privacy Act requires agencies to ensure that a requester is appropriately identified before releasing health / personal info. Here the medical centre made an assumption that N was M and took no steps to verify whether this assumption was correct.

We formed the view the medical centre had breached rule 5 (and rule 11 with regards to disclosure). The medical centre accepted that its procedures were lacking, made extensive changes to its policy regarding the identification of information requesters, and trained its staff in their obligations under the HIPC. The medical centre also reached a settlement with M including an apology, financial compensation, and an agreement about providing M and his children with free medical services for a period of time.
1. Follow the directions of your facilitator to form pairs or small groups.

2. Follow the directions of your facilitator to complete Table 6.

### Security questions

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Would this breach rule 5? Why?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mike</strong></td>
<td></td>
</tr>
<tr>
<td>Mike is a nurse on night-shift. As the ward is quiet, he decides to check the hospital’s database to see if anyone he knows has recently been admitted.</td>
<td></td>
</tr>
<tr>
<td><strong>Katherine</strong></td>
<td></td>
</tr>
<tr>
<td>Katherine, a hospital employee was voluntarily admitted to hospital as a mental health inpatient. Her discharge summary was sent to her home address and the envelope was stamped ‘Mental Health Inpatient Unit’. Katherine was sharing a flat at the time and her flatmates were not previously aware that she had a mental illness. As an employee, Katherine knew that the hospital policy was to delete the name of the department from outgoing mail so the envelope did not disclose the patient’s health condition.</td>
<td></td>
</tr>
</tbody>
</table>

Table 6 - Security questions (rule 5)
Group activity

3. Use the space provided to write any notes or questions.

________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
Data breach

Key question

What is a data breach?

A data breach is when someone who should not have access to personal information sees it, either intentionally or by accident.

Key question

How do data breaches happen?

Data breaches happen in a number of ways, including:

- **lost records and equipment** - lost or stolen laptops, USBs (memory sticks) or paper records
- **incorrect e-waste disposal** - incorrect hardware disposal and return caused by computer hard disk drives being thrown away, recycled or returned to leasing companies, or serviced incorrectly, without the contents first being erased
- **hackers** - illegal access of databases
- **employee browsing** - accessing or disclosing personal information without authorisation
- **document theft** - taken from recycling or rubbish bins
- **information given to the wrong person** - information sent to the wrong physical or email address
- **fraudsters** - releasing personal information to a person pretending to be someone else
Dealing with a data breach

Rule 5 is also the main rule which is engaged when there is a privacy (data) breach. There are four key steps an agency should take when something goes wrong with the personal information it holds.

Key steps: responding to a breach

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Containment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contain the breach and make an initial assessment.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evaluate the risks.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Notification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notify affected people if necessary.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Prevention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevent a repeat.</td>
<td></td>
</tr>
</tbody>
</table>

If you think there has been a breach, move quickly to investigate the breach and what harm it could do.

Think about these questions:

- What could happen to the people the information relates to - i.e., your customers, clients, suppliers, patients, etc.?
- What harm could this do to your organisation - e.g., a loss of public trust and / or damage to the organisation’s reputation?

Steps 1, 2 and 3 should be undertaken either simultaneously (at the same time) or in quick succession (one after the other). Step 4 provides recommendations for longer-term solutions and prevention strategies. The decision on how to respond should be made on a case-by-case basis.

Key point

Every situation will be different, so the response will be different. However, in all cases you must think and act quickly, which includes carrying out the ‘four steps’ as quickly as possible. The Privacy Breach Guidelines are available at www.privacy.org.nz.
Containment / assessment and evaluation of risks

Breach containment and preliminary assessment

Once you have discovered, or suspect, that a privacy breach has occurred, you should take immediate common sense steps to limit the breach, for example:

- **Contain the breach** - Stop the unauthorised practice, recover the records, shut down the system that was breached, revoke or change computer access codes or correct weaknesses in physical or electronic security.

- **Designate an appropriate individual** - Someone should be appointed to lead the initial investigation.

- **Determine who needs to be made aware of the incident** - Decide who should be told what has happened. Escalate internally as appropriate and inform the person within your agency responsible for privacy compliance (typically the privacy officer).

- **Contacting authorities** - If the breach appears to involve theft or other criminal activity, notify the Police.

Evaluate the risks

To determine what other steps are necessary, you should assess the risks associated with the breach. Consider the following factors when assessing the risks:

- **How sensitive is the information?** Generally, the more sensitive the information, the greater the risk of harm to individuals.

- **How can the personal information be used?** Can the information be used for fraudulent or otherwise harmful purposes? The combination of certain types of sensitive personal information along with a name, address and date of birth suggests a higher risk due to the potential for identity theft.

- **To the extent possible, determine the cause of the breach.**

- **Is there a risk of ongoing breaches or further exposure of the information?**
• Has the personal information been recovered?
• What steps have already been taken to mitigate the harm?
• How many individuals’ personal information was affected by the breach?
• What harm could result from the breach? Examples include:
  - a security risk (for example, danger to physical safety)
  - identity theft
  - financial loss
  - loss of business or employment opportunities, and / or significant humiliation or loss of dignity, damage to reputation or relationships

Notification and prevention

Notification

Key question

Should affected parties be made aware of the breach / how will you notify them?

If a privacy breach creates a risk of harm to the individual, they should be notified. Each incident needs to be considered on a case-by-case basis to determine whether a privacy breach notification is necessary. Remember that it is currently voluntary whether you notify anyone of a privacy breach. Agencies are encouraged to inform the OPC of material privacy breaches so that it is aware of the breach and can effectively handle any related enquiries (questions) or complaints.

The key consideration in deciding whether or not to notify affected individuals should be whether notification is necessary in order to avoid or mitigate harm to the individual whose personal information has been inappropriately accessed, collected, used or disclosed. Agencies should also take into account the ability of the individual to take steps to mitigate any harm.
Consider the following factors when deciding whether to notify:

- Do you have any legal and contractual obligations?
- What is the risk of harm to the individual? Is there a risk of physical harm (if the loss puts an individual at risk of physical harm, stalking or harassment), or of identity theft or fraud?
- What is the ability of the individual to avoid or mitigate possible harm?

Notification to individuals affected by the breach should occur as soon as reasonably possible following the assessment and evaluation of the breach. The preferred method of notification is directly to affected individuals by phone, letter, email, or in person.

**Key point**

If a privacy breach creates a risk of harm to the individual, they should be notified.

For more information see the OPC’s Privacy Breach Guidelines and guidance on ‘Finding other people’s personal information’.

**Prevention**

**Key question**

What lessons can be learned from this experience to prevent future breaches?

Agencies need to take the time to investigate the cause of the breach and consider whether to develop a prevention plan. The level of effort should reflect how serious the breach was, whether it involved the whole organisation or just one small part, and whether it would be likely to occur again or whether it was just a one-off event.
Insights for agencies

Make privacy and information security top priorities for your organisation. People need to have confidence that their personal information is protected.

Ensure that workers are getting training on how to respect people’s information, how to manage their data and how to prevent breaches.

Carry out spot audits on what information is being accessed, for what reasons and by whom.

Case note 248601 [2013] NZ PrivCmr 4: medical practice mitigates future harm after data breach

A doctor working in a suburban medical practice had a USB stick containing patient information stolen after his car was broken into. The USB contained information about the complainant including their first and last names, details of prescribed medication and their diagnosis.

The medical practice acted quickly and worked through the four steps described above:

Breach containment - The medical practice received news of the theft the following day and the manager immediately made plans to contact the affected individuals. The complainant (C) was told of the breach by his GP and offered a meeting with the practice manager to discuss the situation.

Evaluation of risks - The manager noted the only identifying information was the name as C had frequently changed addresses and a current telephone number was not listed. The manager believed the main harm was that C may lose faith in the medical practice. However, C has continued to use the medical practice’s services since the breach.

Notification - The patients were notified as soon as reasonably possible. The manager of the practice met with C to discuss the theft and apologised for the loss of C’s health information.
Prevention - The medical practice took steps to increase the security of any data that was to leave the premises. A review was conducted of their patient information security policy and immediate changes were drafted to be signed off by the Board of the practice.

The practice purchased new encrypted USB sticks immediately after the data breach, to be used when taking data off the premises. An active register containing a list of the staff allowed to use the USBs was implemented and an agreement drafted up for staff to sign acknowledging that they are responsible for the safety of the information. Staff were advised verbally and electronically of the new process and the medical practice ensured there was a transparent communication process with the staff about the data breach.

In this case C sought damages as a result of the breach. However, we were not satisfied that he had suffered harm that warranted damages. We also considered that the practice had taken appropriate steps in the circumstances.
Rule 6 - access

Key point

Rule 6

People have the right to ask for access to personal information about themselves.

Agencies can refuse to give access in some limited situations, for instance, where giving the information would:

- endanger a person’s safety
- prevent the detection and investigation of criminal offences, or
- involve an unwarranted breach of someone else’s privacy

Under rule 6 individuals are entitled to:

- know whether an agency holds information about them, and
- access that information if it is readily retrievable

There is a presumption of access. So, if someone asks you for information you hold about them, it is presumed that you will provide it. There are also procedural provisions (what needs to be done and how) that you need to follow, including set timeframes. The procedural provisions are found in parts 4 and 5 of the Privacy Act.

However, the right to access personal information is not absolute and an agency will be allowed to withhold personal information in limited circumstances. These withholding grounds are set out in sections 27-29 of the Privacy Act.

What will be regarded as readily retrievable will depend on the circumstances of the case. What is deemed retrievable may not be limited to written documentation and can extend to discussions.

Whenever an agency provides a decision in response to an information request, it must inform the individual of their:

- right to have the decision reviewed by the Privacy Commissioner, and
- right to request correction of any information they believe is incorrect, under principle 7 of the Privacy Act
Requests

Rule 6 requests - preliminary matters

There are a number of things to keep in mind when dealing with a request for personal information, including the following:

- Requests for information may be in written or oral form and individuals do not have to explain why they want their information.
- A request cannot be refused on the basis that the individual does not own the information. Equally, the right of access is not a right to possess original documentation.
- Information is not limited to written documentation, but can extend to information in the mind of an individual.

Agents

Individuals can voluntarily appoint agents. However, check that they are properly authorised to request access, and that there is written authority and the agent is properly identified (section 45 of the Privacy Act).

Representatives

The Code uses the word representative in only a few places to provide additional protection to the privacy of individuals who may be unable to exercise their rights.

There are three categories of representative:

- where a person is dead, their personal representative (the executor or administrator of their estate)
- where a person is under 16, dead or alive, that person’s parent or guardian (custodial or non-custodial)
- where a person cannot give consent or exercise rights, a person lawfully acting on their behalf or in their best interests. A welfare guardian appointed under the Protection of Personal and Property Rights Act 1988, a person authorised under an enduring power of attorney in relation to personal care and welfare, or a counsel for a child would fall under this category of a representative.
Procedural provisions

Procedural provisions are what must be done by the agency and how it must be done. There is an obligation on an agency to:

- provide assistance
- transfer access requests
- inform the individual of the decision regarding their request
- respond within time limits
- make information available in the form requested

When an agency receives an access request, the Privacy Act means that you must do the following:

- **Provide assistance (section 38 of the Privacy Act)**
  You must assist the individual making the request; this may include redirecting the individual to the appropriate agency, helping them to formulate a request or advising them of what information the agency holds. This also means you should be able to identify when someone is seeking information that they are entitled to request under the Privacy Act, even if they do not directly refer to the Act.

- **Transfer access requests (section 39 of the Privacy Act)**
  Where you do not hold the information, but believe it to be held by another agency, you must transfer the request within 10 working days from receipt and inform the individual accordingly. You can also transfer a request where you do hold the information if the information is held by another agency and it is more closely related to that agency, e.g., where you have received a copy of a report from another agency.

- **Inform the individual of the decision regarding their request (section 40 of the Privacy Act)**
  If you do not transfer the request, you must make a decision in relation to the request and inform the individual of this decision. Your decision should include whether you intend to make the information available in full, in part, or not at all, and if the request is to be granted - the way in which the information will be made available. You must also inform the individual of the basis for withholding any information and their right to have your decision reviewed by the Privacy Commissioner.

You do not have to provide the individual with the information at the same time as you make a decision (although this will generally be the case). However, if you do not provide the information at the same time, you must provide it without undue delay. (What is considered to be ‘undue’ will depend on what the information is and / or whether there is any particular reason for urgency, for instance, if the individual needs the information for an upcoming court case.)
• **Respond within time limits (sections 40-41 of the Privacy Act)**
  Generally, unless you have transferred the request to another agency, you must inform the individual of your decision within 20 working days of receiving the request.

  However, you may extend the timeframe for responding if:
  
  - the request is for a significant amount of information or would require you to search through a large amount of information and this can’t reasonably be done within the original time frame, or
  
  - you need to consult with someone before you can make a decision on the request (for instance, if you need to speak with a specific staff member or another agency) and you are not able to do so and still provide a response within the original time frame

  If you wish to extend the time frame for response you need to tell the individual about this within 20 working days of receiving the request and inform them of:
  
  - the length of the extension, i.e., when you will be providing a response
  
  - the reasons for the extension, and
  
  - their right to make a complaint to the OPC about the extension

• **Make information available in the form requested (section 42 of the Privacy Act)**
  This can be a copy, summary, viewing, etc. The information must be provided in the form requested by the individual unless doing so would impair efficient administration, or be contrary to any legal duty the agency had in respect of the document or prejudice the interests protected in sections 27-29 of the Privacy Act.

---

**Key point**

There is an obligation for an agency to:

- provide assistance
- transfer access requests
- inform the individual of the decision on their request
- respond within time limits, and
- make information available in the form requested

A failure to fulfil these obligations constitutes an interference with the privacy of the individual.
Timeframes for response

There are reasonable timeframes within which an agency must respond to a request. The request may be for access or for correction.

<table>
<thead>
<tr>
<th>Request type</th>
<th>Time limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response or notification of extension</td>
<td>20 working days</td>
</tr>
<tr>
<td>Transfer</td>
<td>10 working days</td>
</tr>
</tbody>
</table>

Table 7 - Response timeframes

Charging

Public health agencies may not charge for making information available.

Private sector agencies may not charge for making information available, unless:

- the agency receives a second request for information within twelve months and the requested information is substantially the same, or
- the charge is in respect of providing a copy of an X-ray, video recording or CAT scan photograph

Where the charge is likely to exceed $30, the agency must provide the individual with an estimate of the charge before processing the request.
Some withholding grounds

The right to access your personal information is a broad right. There are very few situations where it may be legally withheld. These are called **withholding grounds** in the Act, and are discussed below.

An important point to note here is that when you decide to withhold any information you must inform the individual of their right to have that decision reviewed by the Privacy Commissioner. You should also take reasonable steps to keep a record of what information you have withheld and why, and make sure that you retain the information for a reasonable length of time to allow the individual to have the decision reviewed if they want to.

Table 8 shows a limited list of the reasons that an agency may legally not give out personal information.

| Grounds to withhold information from an individual; sections 27-29 of the Privacy Act |
|---------------------------------|---------------------------------|
| Section                        | Title                           |
| Section 27(1)(c)               | prejudice maintenance of law    |
| Section 27(1)(d)               | endanger safety                 |
| Section 29(1)(a)               | unwarranted disclosure          |
| Section 29(1)(b)               | evaluable material, defined in section 29(3) |
| Section 29(2)                  | not readily retrievable / cannot be found / does not exist |

Table 8 - Withholding grounds under the Privacy Act

If release could prejudice maintenance of the law

Under **section 27(1)(c)**, an agency may withhold information if its disclosure would be likely to prejudice the maintenance of the law, including the prevention, investigation or detection of offences. The Police and other agencies with a law enforcement function often use **section 27(1)(c)** as a reason not to release information. It is generally expected that at the conclusion of the investigation the information will be released.

However, in limited circumstances some information may continue to be withheld under this section after an investigation has ended. For example, this may be to protect an informant’s identity and to protect investigative technique (how the information was obtained), etc.
If it may endanger the safety of any individual

Under section 27(1)(d), an agency may withhold information if the disclosure would be likely to endanger the safety of any individual. This means that their physical safety could be compromised (i.e. they would be at risk of harm). If you seek to withhold information on these grounds you must be sure that there is a serious or real and substantial risk, or a risk that may well eventuate.

Rule 6 allows an agency to withhold information in some circumstances. The two grounds in relation to mental health are if disclosure would be likely to endanger the safety of any individual (section 27(1)(d)) or if disclosure would be likely to prejudice the physical or mental health of that individual (section 29(1)(c)). An example of this is illustrated in the following case note.

In a recent HRRT case (Te Koeti v ODHB, HRRT 4/09) the plaintiff requested information about their admissions to the Emergency Department since 1998. Otago District Health Board (ODHB) withheld the names of nurses who had attended the plaintiff under section 27(1)(d).

The plaintiff was well-known to staff at Dunedin Public Hospital (treated the ED like a GP service); presented as a difficult patient and had a history of confrontational and aggressive behaviour. ODHB was concerned the plaintiff wanted the names of nurses and what he might do with that information.

The test for ‘likely’ to endanger the safety of an individual in section 27(1)(d) does not require a threat to be more likely to eventuate than not. But it will ‘be enough if there is a serious, real or substantial risk to a protected interest, a risk that might well eventuate … whether such a risk exists must be largely a matter of judgement’.

The plaintiff gave evidence in the HRRT. HRRT found his evidence about his mental health status was significantly understated; he was capable of intimidation, aggressive outbursts, and had a history that raised legitimate concerns as to how he might conduct himself if he was not in control.

HRRT considered that, after weighing the interests of the nurses in question against the plaintiff’s right to access information, the proper course was not to require disclosure of the names of the nurses to him. The release of their names included a risk that at some future time he could track them down and perpetuate some harm.
If disclosure is unwarranted

Section 29(1)(a) provides a withholding ground where the release of the information would involve the unwarranted disclosure of the affairs of another individual. This section is relevant in cases where the information at hand relates to more than one person and is designed to protect the privacy of other individuals. It is used in cases where, given the circumstances, disclosing the information would be an unwarranted disclosure of another individual’s personal information.

Determining what would be unwarranted involves a balancing exercise between the interests of the individuals involved.

In the past the Commissioner has seen the following factors as relevant:

1. the purpose for which the information was supplied or held
2. the purpose for which the information is requested, and
3. the requester’s prior knowledge

Case note 235239 [2013] NZ PrivCmr 1: dealing with child’s health information when parents are separated

A mother requested her child’s medical file from a medical centre, who declined to supply the information because the father did not want it released. The father and mother were separated and the father had custody of the child. Upon investigation, the Privacy Commission advised the medical centre to release the parts of the file relating to the child, but that it could withhold parts that related to the father under section 29(1)(a). The mother was satisfied with the information released and the Privacy Commission file was closed.
If it may prejudice physical or mental health

Section 29(1)(c) allows information to be withheld if the agency is satisfied that disclosure would be likely to prejudice the physical or mental health of the individual (the requester).

The agency seeking to rely on this ground must consult the requester’s medical practitioner if possible. The medical practitioner does not have to be a doctor (for example, they could be a counsellor or therapist) but they must be someone with an ethical obligation to the requester.

The agency is not obliged to accept the views of the medical practitioner, but must take them into consideration along with other evidence before making a decision. The information requested must relate to the physical and mental health of the requester and the agency must be satisfied that the information in question would prejudice the requester’s health. This is rarely supported because of the requirement for a direct causal link between the information and harm.

Case note: HG v TDHB HRRT 2/09

In HG v TDHB (HRRT 2/09) the individual had long history of mental illness and requested medical notes from a period when he had been admitted for compulsory treatment from Taranaki District Health Board (TDHB).

TDHB offered the individual the opportunity to view the file but the plaintiff wanted a copy (as is his right under section 42 - discussed later). A clinical psychologist who he was seeing at the time requested the file from TDHB and over a few weeks the psychologist went through the files with the individual. No copies of the files were given to the individual and the files were later returned to the TDHB. On returning the files, the psychologist told TDHB that the individual had become fixated about staff members at the DHB and about the content of the files. She asked to be notified before a decision was made to release copies to the individual.

When the plaintiff requested a copy of the file, TDHB refused to provide it under section 29(1)(c) which provides an agency may refuse to disclose information under rule 6 if:

‘(c) after consultation with the individual’s medical practitioner, the agency is satisfied that -

The information relates to that individual and

The disclosure of the information (being information which relates to the physical or mental health of the individual who requested it) would be likely to prejudice the physical or mental health of that individual.’
TDHB consulted with the individual’s psychologist who considered that to provide a copy of the notes would likely have a negative impact on his well-being and could seriously affect his mental health. The individual was described as having a history of impaired understanding with a tendency to develop his own interpretations of information and become negatively fixated on people and events. TDHB was concerned that, if the individual had a copy at home, he would dwell on the information, misunderstand it and that he might act on his mistaken impressions and concerns in a way that could be detrimental not only to himself but to others.

If the information is not readily retrievable

If the information cannot be provided because it does not exist or cannot be found, then you should rely on section 29(2)(b). However, before they rely on this section, they must undertake a reasonable search. The agency also needs to consider that if they are unable to find personal information that they should hold, this may raise issues under rule 5.

Key point

When making information available the agency must take precautions by:

- only making information available where you are satisfied of the identity of the requester (rule 5), and
- ensuring that the individual or their agent receive the information, and
- if an agent is involved, that the agent is properly authorised.
### Group activity

1. Follow the directions of your facilitator to form pairs or small groups.
2. Follow the directions of your facilitator to complete Table 9.

<table>
<thead>
<tr>
<th>Grounds to withhold information from an individual</th>
<th>Section of the HIPC (and Privacy Act)</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>27(1)(c) - prejudice maintenance of law</td>
<td></td>
<td></td>
</tr>
<tr>
<td>27(1)(d) - endanger safety</td>
<td></td>
<td></td>
</tr>
<tr>
<td>29(1)(a) - unwarranted disclosure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>29(1)(b) - evaluative material, defined in section 29(3)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Group activity

<table>
<thead>
<tr>
<th>Grounds to withhold information from an individual</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Section of the HIPC (and Privacy Act)</strong></td>
</tr>
<tr>
<td>29(1)(c) - it may prejudice mental / physical health</td>
</tr>
<tr>
<td>29(2) - not readily retrievable / cannot be found / does not exist</td>
</tr>
</tbody>
</table>

Table 9 - Examples of withholding grounds

3. Use the space provided to write any notes or questions.

________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
A man requested a copy of his medical file from a former healthcare provider. The provider gave him most of the file, but withheld information regarding comments the man’s mother made about him. The mother had since passed away.

Section 29(1)(a) permits an agency to withhold information if releasing it would involve the unwarranted disclosure of the affairs of another individual or of a deceased individual. The provider believed that, given the nature of the comments made by the mother, and the fact that the mother was unable to explain or justify the comments as she had passed away, it would be unwarranted to release the information. Based on the provider’s comments, we were satisfied section 29(1)(a) applied in this case.

Requests under section 22F of the Health Act

Section 22F of the Health Act also allows information requests to be made which then must be processed as if they were requests made under rule 6. There are three parties who can make a request under this section:

- the individual themselves (rule 11(4)(a) provides that it be treated as a request made under rule 6)
- representatives, as defined earlier in this material, and
- any other person or agency that is to provide health services to the individual (i.e., another health care provider)

When an agency receives a request under section 22F, it must disclose information unless it has a proper basis for refusal.

A request by the individual
If the request is made by the individual concerned, look at sections 27-29 of the Privacy Act for reasons you may refuse to disclose information.
A request by a representative
If you receive a request from a representative you may also refuse to provide information if disclosure:

1. would be contrary to the individual’s interests, e.g., abuse by the representative is suspected, or
2. the agency has reasonable grounds for believing that the individual does not, or would not, wish the information to be disclosed, e.g., a patient might be receiving voluntary psychiatric treatment and has stated that he does not want his family to know, or
3. would be prevented because one of the withholding grounds in sections 27-29 would apply if the individual themselves had made the request

For example, a woman contacted the Office stating that her request for access to the medical notes of her mother had been refused. She explained that she had not been in contact with her mother for some time due to a family dispute, but required her mother’s medical notes in order to attempt to get her sectioned. It was at this point that it became apparent that she was not acting in her mother’s best interests and, as such, could not be considered as her mother’s representative.

A request by a healthcare provider
An agency may refuse a healthcare provider’s request under section 22F(2)(a) and (b) if:

• the agency has a lawful excuse not to disclose
or

• the agency has reasonable grounds for believing that the individual does not wish the information to be disclosed

Figure 12 looks at how you can respond to a request under section 22F of the Health Act.

Section 22F Health Act 1956

Upon request the holder of health information must disclose to:

<table>
<thead>
<tr>
<th>Individual</th>
<th>Treat as rule 6, sections 27-29 of the Privacy Act apply</th>
</tr>
</thead>
<tbody>
<tr>
<td>Representative</td>
<td>Agency may refuse if: contrary to individual’s interests or patient veto, or sections 27-29 of the Privacy Act apply</td>
</tr>
<tr>
<td>Healthcare Provider</td>
<td>Agency may refuse if: individual doesn’t want disclosure or there is a lawful excuse not to disclose</td>
</tr>
</tbody>
</table>

Figure 12 - Applying section 22F of the Health Act 1956
A mother had requested her child’s health info from a medical clinic. The clinic had declined to provide the information because the child’s father did not want the information to be released.

Under section 22F of the Health Act, parents and guardians are permitted to request their child’s health information, if the child is under 16 years old. Where an agency receives a request under section 22F, it is required to deal with the request as if the individual was requesting their own information. This means the information must be released unless it has a proper basis to withhold. Information may be withheld where:

- the child does not want the information to be released
- it would not be in the child’s best interests to disclose the information, or
- one of the withholding grounds in sections 27-29 of the Act applies

In this case the clinic advised that the child’s mother and father had separated and that the father had custody of the child. While the clinic was willing to provide the mother with information that was only about the child, it did not want to disclose any information contained in the file relating to the father out of concern for his privacy.

We reviewed the file and formed the view that the majority of the information was about the child and that the mother was entitled to it. However, a small amount was mixed information about the child and the father.

Given the nature of the information and the difficult relationship between the mother and father, we were satisfied it would be unwarranted to provide the mixed information to the mother. The clinic provided the information that was only about the child to the mother and she was satisfied with this.

The flowchart in Figure 13 sets out the procedure which must be followed when responding to a request made under rule 6 or section 22F of the Health Act 1956.
If you have any concerns on how to proceed with an information request, feel free to contact our enquiries team on 0800 803 909 or enquiries@privacy.org.nz.

Releasing Withholding
You need to:
- Advise the requester that you are withholding the information (section 44)
- Set out the relevant withholding ground/s (Privacy Act sections 27-29 or Health Act section 22F(2))
- Advise the requester that they can ask the Office of the Privacy Commissioner to review this decision

You need to:
- Consider how to provide the information (section 42)
- Consider if you want, and are able, to charge for the information (section 35)
- Inform the requester of their right to request correction of the information (principle 7)
- Release without undue delay

Are you going to release the requested information, or do you want to withhold all, or some of it?

If you require more time to process the request, and meet the criteria, you should advise the requester that you require an extension (section 41)

Access to health information under the HIPC

Figure 13 - Access to health information under the HIPC
Rule 7 - correction

Key point

Rule 7

People have a right to ask an agency to correct information about themselves if they think the information is wrong.

If the agency does not want to correct the information, it does not usually have to. But if it does not correct the information, it must give the person the opportunity to add their views about what the correct information is.

Rule 7 provides individuals with the right to request correction of information. When an agency receives a request for correction and it does not want to make that correction, it must inform the individual of three things:

1. the reason for the refusal
2. the individual’s right to request that a statement of correction be attached to the disputed information, and
3. the individual’s right to complain to the Privacy Commissioner

The Code does not say what form a reason for refusal must take. However, there is an obligation under rule 7 to ensure that information is correct. Therefore, the agency may state that the information was the opinion held at the time the information was compiled.

If the agency makes the requested correction or attaches a statement of correction, it is obliged to take two steps:

1. inform any agency which has received the information of any changes made, and
2. ensure that the statement will be read in conjunction with the disputed information
A possibility that you might like to consider, especially where the disputed information is historic, is to separate the disputed information from the file and leave a note in the file as to its existence.

The way your agency must go about responding to correction requests is set out in the Code. The Code calls these **procedural provisions** and they are the same under rules 6 and 7. The procedural provisions state the following:

1. The agency has an obligation to assist the person making the request (**section 38**).
2. The agency must inform the individual of its decision on the request within 20 working days of receiving the request (**section 40**).

![Key point]

Where an agency responds to a request under rule 7 by either making a correction or attaching a statement of correction, it must take reasonable steps to ensure that any other agencies which have received the information are made aware of the correction.

**Individuals have a right to request correction; or have a statement of correction added.**

**Agency must either:**

- make the change
- attach statement

- inform the individual and any recipients of the information

---

**Figure 14 - Individual right to have information corrected**
1. Follow the directions of your facilitator to form groups.
2. Follow the directions of your facilitator to complete the review quiz.
3. Use Table 10 to make any notes.

<table>
<thead>
<tr>
<th>Review quiz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notes</td>
</tr>
<tr>
<td>Question 1</td>
</tr>
<tr>
<td>Question 2</td>
</tr>
<tr>
<td>Notes</td>
</tr>
<tr>
<td>Question 3</td>
</tr>
<tr>
<td>Question 4</td>
</tr>
</tbody>
</table>
## Group activity

<table>
<thead>
<tr>
<th>Review quiz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notes</td>
</tr>
<tr>
<td>Question 5</td>
</tr>
<tr>
<td>Question 6</td>
</tr>
<tr>
<td>Notes</td>
</tr>
<tr>
<td>Question 7</td>
</tr>
<tr>
<td>Question 8</td>
</tr>
</tbody>
</table>

Table 10 - Review quiz
Rule 8 - accuracy

Key point

Rule 8

Before using health information, an agency must take reasonable steps to ensure it is:

- accurate
- up-to-date
- complete
- relevant
- not misleading

What is reasonable will depend on where the information was obtained and when it was obtained. What is reasonable will also depend on the proposed use. This can be particularly important where information has been obtained from a source other than the person concerned. It may be sensible to verify that information with the person concerned.
1. Follow the directions of your facilitator.
2. Discuss the accuracy example (case note 17749).
3. Respond to the questions posed by your facilitator.
4. Use the space provided to write any notes or questions.
An ACC claimant’s attendant care and home help compensation was cancelled after an assessment carried out on behalf the ACC. The claimant was almost completely disabled. There was no likelihood of recovery for the claimant.

During the course of the investigation it became apparent that the assessor had mistakenly attached the wrong assessment to the claimant in which the assessor stated that the claimant enjoyed hanging out the washing and doing the ironing and house work.

The Commissioner found ACC in breach of rule 8. The Commissioner considered that it would have been reasonable in the circumstances to check the assessment with information already held about the complainant. It would also have been reasonable to give the claimant an opportunity to comment on the report because the ACC was considering taking adverse action against him.

Key question

What does accuracy mean?

When the OPC reviews a rule 8 (accuracy) complaint, the review focuses not on the quality of the overall decision made, but on whether or not the agency followed a reasonable process in reaching that decision.
Rule 9 - retention

Key point

Rule 9

Agencies must not keep health information for too long. They can only keep it for as long as is necessary for any lawful purpose of use.

Rule 9 requires that agencies do not retain health information for longer than is required for the purposes for which that information may be lawfully be used. This links with, and provides support to, other rules. It discourages agencies from continuing to hold health information that is no longer needed.

A privacy risk exists where information is retained, because:

- the information may become out of date and therefore should not be used (rule 8)
- the accumulation of information creates a risk that it will be used without regard to the purpose for which it was collected or obtained (rule 10), and
- the retention (holding on to) of information increases the risk that it will be inadvertently disclosed (rules 5 and 11)

Figure 15 - It is important to have a policy on how long information will be kept
Retention times and legal obligations

When health information is no longer required, it can be returned, destroyed or transferred. There are rules around how each should be done. Agencies should have a policy around how to handle health information when it is no longer needed.

There are several issues that an agency must consider when developing a retention policy:

- Should information be retained (kept) at all? (Keep in mind that there may be other laws which require you to keep information.)
- If so, for how long?
- How should any information that is no longer required be disposed of? (rule 5)

The Health (Retention of Health Information) Regulations 1996 require health information to be retained for at least 10 years from the last date of treatment or care unless the information is transferred to another provider or given to the individual. Rule 9 does not override the regulations.

Figure 16 - Regulations require health information to be retained for 10 years from the last date of treatment - rule 9 does not overrule this
1. Complete Table 11 with examples from your agency.

2. Talk to your supervisor or a more experienced workmate where applicable.

<table>
<thead>
<tr>
<th>Managing data at your agency</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Question</strong></td>
</tr>
<tr>
<td>What are some examples of information held by your agency?</td>
</tr>
<tr>
<td>How long do you hold on to this information?</td>
</tr>
<tr>
<td>Why do you keep it for this long? For example, is it necessary in order to comply with legal obligations or is it your agency’s policy?</td>
</tr>
<tr>
<td>What happens to information you no longer need to retain?</td>
</tr>
<tr>
<td>How often are audits conducted to review information?</td>
</tr>
</tbody>
</table>

Table 11 - Managing data at your agency
Rule 10 - use

Key point

Rule 10

Agencies must use health information for the same purposes for which they obtained that information.

Other uses are occasionally permitted (for example, where this is necessary to enforce the law, or where the use is directly related to the purpose for which the agency obtained the information).

The key concept of rule 10 is that health information obtained for one purpose must not be used for another purpose unless the agency believes, on reasonable grounds, that an exception applies. Examples of exceptions are where:

- the other use was authorised by the individual or their representative, or
- the other purpose is directly related to the purpose for which the information was originally collected

Rule 10 is similar to rule 11 - disclosure. Both rules 10 and 11 limit the use and disclosure of information to the purpose for which it was collected or obtained.

Some exceptions to rule 10

Again, non-compliance is permissible in certain circumstances where the agency believes on reasonable grounds that:

- another use is authorised by the individual concerned (section 10(b))
- the other use is directly related to the purpose for which the information was collected (section 10(e))
The agency can use the information for purposes other than the purpose for which it was collected if:

- this is necessary to avoid prejudice to maintenance of the law or the conduct of proceedings before a court or tribunal (section 10(c)(i) and (iv))
- the information is used without identifiers (section 10(f)(i)), or for statistics or research (section 10(f)(ii)), or
- the information is originally sourced from a publicly available publication and, given the circumstances, it would not be unfair or unreasonable to use that information (section 10(a))

These are not the only exceptions, but cover the most common examples. Questions for you to consider before using personal information you have obtained for another use include:

- What was the purpose of collection?
- Was the individual made aware of that purpose?

Case note 211472: [2010] NZPrivCmr 2: woman’s health information released by District Health Board to Ministry of Health

A woman complained her anonymised health information was given to the Ministry of Health by her District Health Board as part of statistical information about events within the DHB, and then published in the local paper as part of a report on the DHB. She felt the information published could identify her. The case was reviewed and her complaint was not upheld, citing section 22(H) of the Health Act (this section specifically permits the disclosure of health information where the information has been anonymised).
Rule 11 - disclosure

Key point

Rule 11

Unless another law overrides the HIPC, health agencies must not disclose personal information unless an exception applies. An agency can disclose information if it reasonably believes, for example, that:

- disclosure is one of the purposes for which the agency obtained the information
- disclosure is necessary to uphold or enforce the law
- disclosure is necessary for court or tribunal proceedings
- the person concerned authorised the disclosure, or
- the information is going to be used in a form that does not identify the person concerned

Disclosure of health information can become an issue in cases where you have been asked for information about an individual by a third party or in any other case where you want to disclose information about an individual.

Rule 11 provides that an agency must not disclose personal information unless it believes, on reasonable grounds, that an exception applies. The exceptions discussed below are not the only ones, but cover the most common examples.

It is important to note here that disclosure under rule 11 is discretionary - this means that it is the choice of the agency (even if an exception applies). Also remember that if you do disclose information, you should take care to avoid ‘over-disclosure’ by only disclosing the necessary information.

Also keep in mind that there may be cases where you are required to disclose personal information, for example, if Police obtain a search warrant or if a court has ordered discovery. Because you are required to disclose this information under another law, this overrides rule 11.
Key point

Rule 11(1) allows disclosure

Rule 11 of the Code is the bottom line for disclosure (unless another law applies). If you cannot disclose information under rule 11, then don’t do it.

Must disclose

An agency may have to disclose health information because it is required to do so by law. This is covered in section 7 of the Privacy Act. Any law which requires or authorises disclosure takes priority over the Code (and the Act).

- Mandatory key words are words like ‘shall’ or ‘must’, or phrases such as ‘is required to’.
- Generally, there is nothing to prevent an agency from telling the individual that the disclosure will have to be made. Where disclosure is anticipated, this should be done when giving the rule 3 statement.
- Health professionals should also ensure that any disclosure they make complies with their Code of Ethics. Many Codes of Ethics will allow disclosure if it is required by law. If in doubt, you should check with your professional body.

Examples of statutes that require disclosure include:

**Cancer Registry Act 1993, sections 5 and 6**

Requires disclosure of a positive cancer test by a person in charge of a testing laboratory to the Director General of Health.

**Land Transport Act, sections 18 and 19**

Requires registered medical practitioners and optometrists to notify the New Zealand Transport Authority (NZTA) if they consider a patient is likely to drive and whose medical / mental condition is such that in the interests of public safety that person should not be allowed to drive. **Section 19** requires a person in charge of a hospital to notify the NZTA if a patient who holds a licence becomes the subject of a compulsory treatment order so that their licence can be suspended.

**Mental Health (CAT) Act 1992, section 7A(2)**

**Section 7A(2)** requires medical practitioners to consult with family and whānau when sectioning or considering whether to section a patient.
Health and Disability Commissioner Act, section 62 (also section 91 of the Privacy Act)

The Health and Disability Commissioner can require a health or disability provider to make information available for an investigation. The Privacy Commissioner has similar powers under section 91.

Tuberculosis Act 1948, section 3

This Act requires medical practitioners to notify a Medical Officer of Health if they believe a patient has tuberculosis (TB).

Medicines Act, section 29

Sets out reporting requirements in relation to the sale of certain types of medicines. In these cases suppliers must report the sale to the Director-General in writing, naming the practitioner and patient, describing the medicine, and identifying when and where the medicine was sold or supplied.

Social Security Act, section 11

The Social Security Act has broad powers, and it can require anyone to provide anything. There are some limitations though, as it is subject to a Code of Conduct. Requests under this Act must be in writing, and should refer to the Act and its relevant section. The agency then has five days to provide the information.

Children, Young Persons & their Families Act 1989, section 66

You may receive a request about a patient under this Act. These requests are usually in relation to a care and protection issue. Requests under this Act are subject to the 20 working day rule if someone asks you to disclose.

You may be asked to disclose information because:

- Police are investigating an offence
- media are following a story
- a social worker is investigating a case of suspected abuse, or
- a family wants information about a relative receiving treatment

Some statutes allow disclosure, but only if a request has been received beforehand. An agency cannot disclose in reliance on these statutes unless it has received a request. This means that you must have a request in order to release the information.
Official Information Act (OIA)

The OIA requires disclosure upon a request being made unless a withholding ground applies. Section 9(2)(a) provides that information can be withheld if it is necessary to protect the privacy of an individual, including that of a deceased person. This requires a balancing exercise between the privacy interests of the individual and the public interest in disclosure.

Key question

The OIA only applies to public sector agencies. Is your agency a public sector agency?

If you receive a request for information from someone who is not:

1. the individual concerned or their agent, or
2. the individual’s representative

and you are a public sector agency, you must consider the request under the OIA.

The request does not have to be in writing. However, ask for it in writing to eliminate any disputes at a later date.

If the information is not held by your agency, but you know which agency does hold it, the request must be referred to them.

Key point

There is a distinction between provisions which require disclosure and those that allow disclosure. If the provision allows disclosure, you may refuse. For example section 22C of the Health Act allows disclosure to specific agencies, but section 22F requires disclosure (unless grounds for refusal apply).
Section 22C Health Act 1956

Section 22C (page 95 of the HIPC) allows disclosure to specific people, but only if the request is received from a member of one of the following groups (who are working in their official capacity):

- medical officers of penal institutions
- probation officers
- social workers
- care and protection co-ordinators
- Police officers

The list at 22C is exhaustive. Check to ensure your requester is a member of one of the groups listed. The list is in the Health Act and on page 69 of the HIPC.

When you receive a 22C request, you have a choice as to whether to provide the information requested. However, information cannot be volunteered under section 22C. There must be a request first.

Key point

Information cannot be volunteered under section 22C of the Health Act. There must be a request from a member of one of the approved groups.
Wanting to disclose

The third category is where you have information and want to disclose it.

If the information does not contain details about an identifiable individual there will not be a privacy issue. If that information is present, then look for a law which authorises or allows disclosure. Such laws will use words such as ‘may’. However, be aware that while a law may authorise disclosure, your professional body or Code of Ethics may limit disclosure.

Some laws allow disclosure:

**Children, Young Persons and their Families Act 1989, sections 15 and 16**

Anyone who believes that a child or young person is at risk of harm, ill-treatment, abuse, neglect, etc., can report the matter to a social worker or the Police. This provision does not require disclosure, but permits it. **Section 16** protects professionals from civil, criminal or disciplinary proceedings if they were acting in good faith.

**Protected Disclosures Act 2000**

Permits disclosure where there is 'serious wrong doing'. It would cover instances where a clinician may be concerned about a patient’s release or where an employee of a residential care facility is seriously concerned about the treatment being provided. The Act provides immunity from civil and criminal proceedings. However, in order to get that protection certain steps must be followed:

1. The information to be disclosed must be about a **serious wrongdoing** as defined by the Act, e.g.: an act, omission, or course of conduct that constitutes a serious risk to public health or public safety.

2. The disclosure must be made in accordance with internal procedures or to an appropriate authority in certain circumstances.

### Key point

While a law may allow disclosure, there may be ethical and / or contractual obligations which prevent disclosure.
An ACC claimant was receiving compensation due to a physical illness. However, following an assessment, a specialist advised ACC that there was no objective evidence for the physical illness and raised the question of fictitious disease or other psychological diagnosis.

ACC asked an independent assessor to undertake a case review. This person agreed it was possible the claimant had a psychological disorder. ACC advised the claimant that a psychiatric assessment was needed and provided him with two psychiatrists to choose from. The claimant agreed to see a psychiatrist and ACC then released relevant information about the claimant to the psychiatrist. ACC did not release the claimant’s complete file.

The claimant complained that he had only consented to see the psychiatrist but did not consent to his health information being disclosed to the psychiatrist.

ACC relied on rule 11(1)(c) of the HIPC which provides health information may be disclosed if disclosure is one of the purposes in connection with which the information was obtained. This includes instances where information is required for further treatment or assessment.

ACC provided the information to the psychiatrist so they could undertake a psychiatric assessment and determine treatment. This was directly related to the purpose for which the information was collected.
Some exceptions to rule 11

If no other law applies, then you must consider whether you can disclose health information under rule 11 of the Code.

Rule 11 is divided into two parts. **Rule 11(1)** deals with **anticipated disclosures** and permits disclosures in certain situations. Anticipated disclosures are those disclosures which were foreseen at the point of collection and which the individual was informed of in accordance with rule 3. They may include such disclosures as an agency’s discharge policy. Consequently, where a disclosure is anticipated there is no need to obtain the patient’s authorisation.

**Key point**

The individual cannot veto an agency’s purpose. In order to take advantage of rule 11(1) an agency must set its purposes for collecting information at the outset and inform the individual of those purposes. This will require an agency to consider why it collects information and to whom it would normally be disclosed. For example, your agency may have a policy of disclosing information to family members or friends who are involved with the treatment of a patient. The patient must be told about any disclosure policies in compliance with rule 3.

Rule 11, **section 1** provides that an agency must not disclose information unless it believes on **reasonable grounds** that:

- **11(1)(a)** - disclosure is to the individual or their representative
- **11(1)(b)** - disclosure is authorised by the individual or their representative where the individual is dead or unable to exercise their rights under the Code
- **11(1)(c)** - disclosure is one of the purposes in connection with which the information was obtained. This exception is important, as it is recognised that disclosures can form part of an agency’s regular procedures.
- **11(1)(d)** - the source of the information was a publicly available publication and that, in the circumstances, it would not be unfair or unreasonable to disclose the information. However, the agency must have **actually** sourced the information from a publicly available publication; it is not enough that they **could have**.
- **11(1)(e)** - the disclosure is information in general terms concerning the presence, location, condition and progress of the patient in a hospital - subject to patient / representative veto
• 11(1)(g) - the disclosure is of the fact of the release from compulsory status under the Mental Health (Compulsory Assessment and Treatment) Act 1992 to the principal caregiver. Check who that person is when collecting information.

Rule 11(2) deals with unanticipated disclosures and recognises that sometimes it is not desirable or practicable for agencies to obtain the patient’s authorisation to disclose information, as the patient may be unconscious, incompetent or refused authorisation.

Rule 11(2) provides for 11 different situations. The five which arise most often are detailed below.

Remember that while rule 11(2) allows disclosure, it is subject to rule 11(3), which states that disclosure is only permitted to the extent necessary for the particular purpose of the disclosure.

Rule 11(2) provides that compliance with rule 11 is not necessary if an agency believes on reasonable grounds that it is not desirable or practicable to obtain the patient’s authorisation and:

• 11(2)(a) - disclosure is a directly related purpose in connection with which the information was obtained
• 11(2)(b) - disclosure is to a person nominated by the individual
• 11(2)(c) - disclosure is in a form which will not identify the individual
• 11(2)(d) - disclosure is necessary to prevent or lessen a serious threat to public health or safety, or the life or health of any individual, including the patient. There are a number of conditions to satisfy in order to rely upon this exception:
  - the threat must be serious
  - the threat must be to the public health / safety or the life / health of the individual, and
  - information must be given to someone who can act to prevent or lessen that threat

The term ‘serious threat’ is defined in section 2 of the Privacy Act and means a threat that the agency reasonably believes to be serious having regard to the following:

a) the likelihood of the threat occurring (what are the chances this will happen), and

b) the severity of the consequences if the threat does occur (how bad would it be), and

c) the time at which the threat may occur (when will it happen)

• 11(2)(i) – disclosure is necessary to avoid prejudice to the maintenance of the law, or for the conduct of court or tribunal proceedings (section 59 of the Evidence Act 2006 limits any disclosure to proceedings in which the sanity, testamentary capacity, or legal capacity of the patient is in dispute).
A GP had a patient who drove a school bus. The patient had a heart condition. The GP
was concerned about the safety of the passengers and told another patient about his
concerns and attempted to organise a petition to have the driver barred from driving
passenger vehicles.

- The disclosure was unlikely to prevent or lessen the threat because it was not
made to the appropriate authority.

- The GP should have informed the NZTA, disclosing in accordance with the Land
Transport Act, which would not have breached the Code.

- In this instance the GP had information and wanted to disclose, but did not look
for a law which permitted disclosure.
Following an aborted suicide attempt, a 23-year-old man sought help from his doctor who prescribed anti-depressants and referred him for assessment by community mental health services. It took a week before he was referred to a counsellor and he was not seen by a psychiatrist.

Three days later he was admitted to hospital after harming himself, but was discharged the following day and died two days later. The man had told the District Health Board (DHB) that he did not want his family to be told of his admission or that he was self-harming.

The Health and Disability Commissioner (HDC) investigated (report released February 2009). In terms of privacy the HDC, Ron Paterson, said the man’s family should have been told about his depression and suicide attempts. The DHB had considered the man was low-risk which Paterson said was a ‘dubious’ assessment due to several suicide attempts in a short period and no proper psychiatric assessment having been done.

The HDC said there should be a low threshold of notifying family of the risk of self-harm and in this case the DHB should have told the man’s family about his mental health problems under rule 11(2)(d)(ii) of the HIPC (to prevent serious or imminent risk to life).

There was no evidence of estrangement from his family, and the man had no other social support.

**Sometimes an individual’s safety should override his or her privacy, and family or caregivers should be involved to help provide a safe environment for recovery.**

**Key point**

Safety trumps privacy; if you have concerns that an individual may hurt themselves or others, tell someone who can do something about it (e.g., the Police).
Figure 17 shows a simple way to tell which laws apply and to help decide if disclosure is required or justified.

**DISCLOSING HEALTH INFORMATION ('HI') UNDER THE HEALTH INFORMATION PRIVACY CODE ('HIPC')**

1. **When you have received a request for HI from anyone other than the individual concerned or their representative**
   - **Are you required to release the HI?**
     - Some laws place agencies under an obligation to report certain information, e.g. section 18 of the Land Transport Act 1998 and the Cancer Registry Act 1993
     - **Yes**
     - **No**

2. **Disclosure of HI when you have not received a request**
   - **Are you required to release the HI under another piece of law?**
     - Some laws permit disclosure in specific circumstances or for specific reasons, e.g. sections 15-16 of the Children, Young Persons and Their Families Act 1989 or the Protected Disclosures Act 2000.
     - **Yes**
     - **No**

3. **Where another law specifically requires disclosure, this overrides the HIPC. You can disclose the HI.**
   - **Yes**
   - **No**

4. **Are you allowed to release the HI under another law?**
   - In some cases you have the discretion to disclose information, but only if you have received a request first, e.g. section 22C of the Health Act 1956 and the Official Information Act 1982
   - **Yes**
   - **No**

5. **Is there another law which allows you to disclose this information?**
   - Some laws place agencies under an obligation to report certain information, e.g. section 18 of the Land Transport Act 1998 and the Cancer Registry Act 1993
   - **Yes**
   - **No**

6. **If you want to disclose this information, you may do so.**
   - **Yes**
   - **No**

7. **You will need to consider disclosure under rule 11 of the HIPC.**
   - **Does an exception under rule 11 apply in the circumstances?**
     - Some exceptions allowing for disclosure under rule 11:
       - Where disclosure is one of the purposes which you collected the information for, or disclosure is directly related (rules 11(1)(c) & 11(2)(b)).
       - If the individual consents to disclosure (rule 11(1)(b)).
       - Disclosure is necessary to avoid prejudice to the maintenance of the law, or for court or tribunal proceedings (rules 11(2)(i)).
       - Disclosure is necessary to prevent or lessen a serious threat (having regard to likelihood, severity and imminence) (rule 11(2)(d)).
     - **Yes**
     - **No**

8. **You can disclose the information, if you want to.**
   - **Make a note of what was released and why**
   - **Do not disclose the information.**

*While it won’t raise issues under the HIPC, before choosing to disclose HI you may also need to consider whether there are any ethical issues with disclosure.

If you have any questions or concerns about disclosing health information, feel free to contact our enquiries team on 0800 809 909 or enquiries@privacy.org.nz for guidance.

---

**DISCLOSING HEALTH INFORMATION UNDER THE HIPC**

---

**HEALTH 101: AN INTRODUCTION TO THE HIPC**

---

103
Key point

If you want to disclose information

If you want to disclose information, look for a law that requires you or allows you to do so.

Otherwise look to rule 11 of the Code. If you are unable to fit within the exceptions available there, do not disclose.

Sometimes it may be an ethical restraint that prevents you from disclosing information. If this is the case, say so.

Case note 228235 [2011] NZ PrivCmr 7: man complains about nurse disclosing health information to a mutual friend

A man was donating blood. During a conversation with the nurse taking his blood he established they had a mutual friend. The man asked the nurse to pass on his regards to the friend.

The nurse passed on the man’s regards, telling the mutual friend they had met when the man was donating blood. The friend then told the nurse of some information about the man which was relevant to whether he was a suitable blood donor. The nurse relayed this information to the blood collection agency, which wrote to the man and told him that it no longer considered him to be a suitable blood donor.

The man complained about the nurse disclosing the fact he had been donating blood. We did not agree that the nurse had breached rule 11 in this case. We considered it was reasonable for the nurse to believe that, because the man had asked the nurse to pass on his regards to their mutual friend, the man would also have been happy for the nurse to tell the mutual friend the circumstances under which they met.

We closed our file on the basis the nurse had not breached the HIPC.
Case note 228129 [2012] NZ PrivCmr 6: sensitive health information disclosed

An ACC claimant had two claims - a sensitive injury claim relating to sexual abuse and a current physical injury claim. The claimant was referred to a physiotherapy clinic and a career assistance agency. Information about his claim was sent to these agencies by ACC.

The man became aware that information about his sensitive claim had been included with the information regarding the injury claim without being appropriately blacked out.

ACC conducted an internal investigation into the matter and accepted that it had breached rule 11 by disclosing information to both agencies which was unnecessary for their purposes and extremely sensitive.

The complaint was resolved by ACC assigning a new case manager, providing a written apology and compensation.

Case note 235915 [2012] NZ PrivCmr 5: a hospital employee disclosed health information about a woman to a mutual friend

A woman was being treated for a serious illness at her local hospital. Her doctor dictated a file note about the woman’s illness and proposed treatment. This was transcribed by an employee of the hospital who was a close friend of the woman and who was able to identify the woman from the dictation. The hospital employee subsequently told a mutual friend about the woman’s illness. The mutual friend then contacted the woman to express their concern.

The woman had not told anyone of her illness at that point, and was very upset that health information about her had been disclosed.

We did not consider any exception applied and the hospital agreed. It accepted that its employee had breached rule 11 and caused emotional harm.

The complaint was settled by the hospital providing the woman with an apology for the stress its employee had caused as well as financial compensation.
1. Follow the directions of your facilitator to form pairs or small groups.
2. Follow the directions of the facilitator to complete Table 12.

<table>
<thead>
<tr>
<th>Disclosure questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anticipated disclosures</td>
</tr>
<tr>
<td>Some general practices keep details of people they believe are drug seekers. This information is passed to other practices to warn of a particular person. It is unlikely that this person would agree to this information being passed on.</td>
</tr>
<tr>
<td>1. Would this disclosure breach the Code?</td>
</tr>
<tr>
<td>2. Could a patient veto the disclosure of the information?</td>
</tr>
<tr>
<td>3. What other issues should the general practice take into account to comply with the Code and with their ethics?</td>
</tr>
</tbody>
</table>
### Disclosure questions

#### Dealing with requests by families and friends

You are treating a person with bipolar affective disorder. She has agreed to the disclosure of information about her condition and medication to her husband, who is to help manage her treatment regime. She has not said anything about disclosure to other people.

The patient’s parents and siblings come to your office and ask for details about her illness, her treatment and prognosis.

<table>
<thead>
<tr>
<th>1. Is this disclosure required or authorised by law?</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Would this disclosure breach the Code?</td>
</tr>
<tr>
<td>3. Are there ways in which the family could be given some information without breaching patient confidentiality?</td>
</tr>
</tbody>
</table>
The Police are investigating a series of sexual offences believed to be committed by one man. They write to every medical practitioner in the greater Auckland region asking for any information which might lead to the apprehension of the offender. A practitioner believes that one of her patients might be the offender.

1. Is there any law authorising the practitioner to disclose to the Police in response to this request?

2. What if the Police had not written to medical practitioners asking for this information? Would the practitioner still disclose to the Police?

3. What limitations, if any, are placed on the practitioner as to the information she could disclose?

Table 12 - Disclosure questions
3. Use the space provided to write any notes or questions.
1. Follow the directions of your facilitator to complete the activity.

2. Discuss the questions asked by your facilitator and refer to the Code where necessary.

3. Use the space provided to write any notes or questions.
Self-check activity

1. Use Table 13 to reflect on how sensitive information is handled at your agency.

2. Talk to your supervisor or more experienced workmate where applicable.

<table>
<thead>
<tr>
<th>Mental health information disclosure</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Question</strong></td>
</tr>
<tr>
<td>When might we need to disclose information to lessen a serious threat to public health or safety?</td>
</tr>
<tr>
<td>In what cases may we be justified to refuse a client access to their own records?</td>
</tr>
</tbody>
</table>

Table 13 - Mental health information disclosure reflection
Rule 12 - unique identifiers

Key point

Rule 12

Some agencies give people a unique identifier instead of using their name. Examples are a driver’s licence number, a student ID number or an IRD number.

An agency cannot use the unique identifier given to a person by another agency. People are not required to disclose their unique identifier unless this is one of the purposes for which the unique identifier was set up (or directly related to those purposes).

An important exception in the health context is the National Health Index Number (the NHI Number). The NHI number is a unique identifier which can be widely assigned and used (see rule 12(3) and Schedule 2 of the HIPC.)

A unique identifier is an identifier that is assigned to an individual by an agency for the purpose of its operations to uniquely identify the individual in relation to that agency.

Rule 12 restricts the use of unique identifiers. An agency may only assign a unique identifier if:

- this is necessary to enable it to carry out its functions, and
- the person’s identity is clearly established

Rule 12 is written this way to lessen the risk that a ‘de facto universal identifier’ will emerge (consider the situation in America where the Social Security Number (along with name and date of birth) is considered proof of identity). If the same number is used across all agencies, there are risks that people’s information may be compromised, and identity theft will be easier and do more damage. If fraud and damage of information occurs, this will affect individual privacy.
There are four parts to rule 12:

1. Agencies are not to assign unique identifiers unless it is necessary to enable them to carry out their functions efficiently.
2. Agencies cannot use a unique identifier that has been assigned by another agency.
3. When an agency assigns a unique identifier, it must take reasonable steps to ensure that unique identifiers are only assigned to individuals whose identity is clearly established.
4. You cannot require an individual to disclose their unique identifier, unless the disclosure is one of the purposes in connection with which that unique identifier was assigned (or a directly related purpose).

**National Health Index Number (NHI Number)**

While the NHI number is an example of a unique identifier, because of the nature of health information, and the need for different health agencies to ensure they correctly identify an individual in order to treat them, the Code permits the NHI Number to be assigned and used more broadly than other unique identifiers. Public hospitals remain the main user of the NHI number, but rule 12 allows some other health agencies to assign the NHI in their transactions with people, such as:

- the Ministry of Health
- licensed hospitals
- registered medical practitioners
- Royal New Zealand Plunket Society
- Blood Transfusion Service, and
- ACC

For more information about this see **rule 12(3) and schedule 2 of the Code**.

**Key point**

An agency must not use identifier assigned by another agency (the NHI number is an exception).
Internal complaints process

Key point

Clause 7 of the Code requires agencies to put in place a process for responding to complaints about breaches of the HIPC.

Health agencies are required to:

- designate someone to deal with complaints about alleged breaches of the Code
- acknowledge the complaint within 5 working days (unless the complaint is resolved)
- make a decision on how the complaint will be dealt with, within 10 working days of acknowledging it

Health agencies must designate a person or persons to deal with complaints about alleged breaches of the Code and to facilitate the fair, simple, speedy and efficient resolution of complaints. The agency must also put in place a process for responding to such complaints.

When an agency receives a complaint about a breach of the Code it is required to acknowledge the complaint and then provide a decision on how the complaint will be dealt with.

Acknowledgement

When an agency receives a complaint and is unable to resolve it directly, within 5 working days it must:

- acknowledge the complaint in writing, and
- inform the complainant of any relevant internal and external complaints procedures

The agency must also ensure that the complaint and the actions of the agency regarding the complaint are documented.
Decision

Within 10 working days of acknowledging the complaint the agency must decide whether it:

a) accepts that the complaint is justified
b) does not accept that the complaint is justified, or
c) needs more time to investigate (in which case the agency must determine how much longer it needs. If it requires longer than 20 working days, it must advise the complainant of this and explain why the extension is required).

As soon as practicable after the agency has decided whether or not it accepts that a complaint is justified, it must inform the complainant of:

a) the reasons for the decision
b) any actions it proposes to take
c) any appeal procedure the agency has in place, and
d) the right to complain to the Privacy Commissioner

There are a limited number of health agencies which are not required to put in place the process outlined above. For instance, it does not apply to agencies which regulate health professionals or district inspectors appointed under the Mental Health (Compulsory Assessment and Treatment) Act. For more details see clause 7(3) of the Code.
Interference

When an individual complains to the OPC that their privacy has been breached, the legal test to be met is whether there has been an interference with privacy (section 66).

The test will be slightly different depending on the type of breach the individual is complaining about.

For a complaint about access to or correction of health information, simply breaching the Code will result in an interference with privacy. For all other complaints, an interference with privacy will require that there has been a breach of the Code and the breach caused harm of the type required under the Privacy Act as a result.

Complaints about information privacy requests

Key point

Requests for access to or correction of health information under the Act are referred to as information privacy requests.

Because the rights of access and correction are such important rights, they are treated slightly differently from the rest of the Code in terms of complaints (section 66(2)).

This means that for information privacy request complaints there will be an interference with privacy where there is no proper basis for a decision on a request, including:

- refusal to make information available
- failure to comply with procedural provisions
- the manner in which information is made available
- undue delay in making information available
- imposing conditions on the use of information made available
- failure to respond within 20 working days
- charging more than allowed (or at all if a public sector company)
- refusal to correct or attach a statement of correction if requested to do so
In the Office it is called an **automatic interference** if you have no proper basis for your decision or you failed to adhere to the procedural provisions. This is why it’s important for your agency to have a clear process for responding to information privacy requests.

This ‘automatic interference’ also applies to rule 7. If an agency refuses to allow correction (or an attached statement of correction) to a file, there is deemed to be an automatic interference. This means the requester does not have to show that any harm occurred. The fact that this was not done is enough.

### All other complaints

![Key point]

**For all other complaints about breaches under the Code (breaches of rules 1-5 and 8-12) the test for an interference is breach and harm.**

According to the Act, an ‘interference with an individual’s privacy’ can be defined as a breach of a privacy principle or Health Code rule and an adverse consequence (**section 66(1) of the Privacy Act**).

Generally there will be an interference with privacy if:

1. an action breaches a rule, and
2. there are adverse consequences

This is the case for rules 1-5 and 8-12. Harm must flow from the breach. As set out above, this does not apply to access and correction requests (rules 6 and 7).

### Adverse consequence

The adverse consequences (what is meant by ‘harm’ as the result of a breach of the Act) are found in **section 66(1)(b) of the Privacy Act**.

To be considered ‘adverse consequences’, the breach must have led to (or may lead to):

- financial loss or other injury
- an adverse effect on a right, benefit, privilege, obligation or interests, or
- significant humiliation, significant loss of dignity, or significant injury to the feelings of the individual
An interference with an individual’s privacy:

for information privacy request complaints (rules 6 and 7)
breach = automatic interference

for all other complaints (rules 1-5 and 8-12)
breach + adverse consequence = interference

The harm must be significant. The interference is important because if the OPC finds an interference with privacy they can refer the matter to the Director of Human Rights Proceedings to consider whether court action is warranted.
1. Follow the directions of your facilitator to form groups.
2. Complete Table 14.
3. Justify your answers. Think about:
   - What rules (if any) have been breached?
   - What harm has been caused?

### Interference questions

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Has there been an interference with privacy? (Explain your answers.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fred wrote and asked his doctor for a copy of his complete medical file.</td>
<td></td>
</tr>
<tr>
<td>a) 32 days later he still had not heard anything from the doctor about his request.</td>
<td></td>
</tr>
<tr>
<td>b) On the 33rd day Fred received a letter from the doctor which stated that Fred could come and look at his file, but only with the doctor present.</td>
<td></td>
</tr>
<tr>
<td>Scenario</td>
<td>Has there been an interference with privacy? (Explain your answers.)</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------</td>
</tr>
<tr>
<td>Sharon’s medical file is accidentally left in the waiting room of the GP surgery.</td>
<td></td>
</tr>
<tr>
<td>a) The practice nurse discovers it and locks it away.</td>
<td></td>
</tr>
<tr>
<td>b) What if Sharon’s neighbour happened to be in the waiting room, and picked it up with the magazines while she was waiting. She could have read the file (or parts of it) and then informed Sharon’s other neighbours and friends about her medical history?</td>
<td></td>
</tr>
<tr>
<td>A doctor disclosed health information about an adult daughter to her mother (an adult is anyone over 16 years of age). Both women are patients of the doctor at the time of the disclosure. The disclosure by the doctor was in response to a specific request by the mother for information about her daughter.</td>
<td></td>
</tr>
</tbody>
</table>
4. Use the space provided to write any notes or questions.
The complaint intake process is as follows:

1. **An individual makes a written complaint**
   The complaint intake process begins with a letter or email from an individual alleging that an interference with their privacy has occurred.

2. **OPC makes an initial assessment**
   Complaints are initially assessed to determine whether the Privacy Commissioner has jurisdiction to investigate the complaint.

3. **The OPC may need to refer the complaint**
   The Commissioner only has jurisdiction to investigate a complaint if it concerns personal information. It may be necessary to refer the complaint to the Office of the Ombudsmen if the complaint involves official information. Or the complaint may be referred to other agencies if it is more appropriate, for example, the Health and Disability Commissioner or the Banking Ombudsman.

4. **The OPC may decline to investigate**
   If the issue complained about has already been canvassed and no breach has been found or the complainant has not suffered any adverse consequences, the Commissioner may decline to investigate the matter. The Commissioner may also decline to investigate if the matter complained about occurred too long ago for an investigation to be desirable or practicable, or if the person making the complaint does not have sufficient interest in the subject of the complaint (e.g., they are not complaining about their own information).

5. **The Investigations Team assesses the complaint**
   If the Office does have jurisdiction and new issues are raised, then the file is looked by the Investigations Team.

This entire process is simplified in Figure 18.
Figure 18 - OPC complaint intake process

Complaint allegations breach of Privacy Act or Code

Does the Privacy Commissioner have jurisdiction?

- Yes
  - Complaint considered by Investigations Team and assigned to an Investigator

- No
  - Complaint transferred or declined
Complaints process

When a complaint is investigated by the OPC, it follows the steps detailed below.

**Assessment**
When the complaint is assigned to an investigating officer, they will begin by assessing the complaint and deciding whether they need further information. They may call, email or write to the individual to request more detail.

**Notification**
Once the investigator considers they have sufficient information they will then notify the agency the complaint is against and invite them to comment. The investigator may decide that it would be helpful to meet with one or both of the parties to the complaint. If necessary the investigator may call a compulsory conference which both sides are required to attend for the purposes of clarifying the complaint and attempting to reach a settlement.

**Settlement is encouraged**
One of the main roles of the OPC is to assist in facilitating the settlement of complaints. As such, throughout the investigation the OPC will consider whether settlement is possible and will encourage the parties to settle, where appropriate.

Settlements will differ from case to case and may include an apology, an assurance against repeating the action which led to the complaint, a change of process, or compensation. However, the parties are free to be as creative as they like when trying to reach a settlement, so the OPC has seen some fairly inventive settlements, including things like gift vouchers, flowers and fruit!

**If no settlement is reached**
If the parties do not settle then a preliminary view is formed. This is not the final decision, but gives an indication to the individual and / or the agency of how the decision may go. This goes to the party the OPC is finding against (the person for whom the decision did not go their way). Sometimes it may be a split primary view, with some issues going to one party and some to the other. The parties have a right of reply.

After parties have responded to a preliminary view, a final view will be formed on the matter.

If a complaint with substance (e.g., there has been an interference) is still not settled satisfactorily, the Commissioner has the discretion to refer the complaint to the Director of Human Rights Proceedings, who may decide to bring proceedings in the Human Rights Review Tribunal (HRRT).
If the OPC do not refer
If the OPC do not refer, the complainant may take proceedings before the HRRT themselves. The difference is that if the OPC refers the complaint, it will be liable for any costs incurred if the case is not successful. However, if the individual takes the case themselves and is unsuccessful, they will have to make a contribution to the costs incurred by the other party.

Reasons why the OPC may, or may not, refer include:
- a reasonable settlement was offered and refused
- availability of proper alternatives to the HRRT
- the seriousness of the complaint
- the behaviour of the respondent agency
- evidential insufficiency
- precedent setting

Human Rights Review Tribunal powers
The HRRT has the same powers as a District Court and can award various remedies including damages of up to $200K. The individual or agency can appeal the HRRT decision to the High Court, then the Court of Appeal, all the way to the Supreme Court.

Damages
To date the most awarded for a breach of the Privacy Act in the HRRT is $40K. However, larger settlements than this have been reached through the OPC.

The full complaints process is simplified in Figure 19.

Figure 19 - Complaints process
Key point

For further information www.nzlii.org is a very useful website for previous Tribunal decisions.
Group activity

1. Follow the directions of your facilitator to form groups.
2. Complete the task as directed by your facilitator.
3. Use the space provided to write any notes or questions.
This list shows some of the words that have been used, and what they mean in this workbook.

<table>
<thead>
<tr>
<th>Word</th>
<th>What it means in this workbook</th>
</tr>
</thead>
<tbody>
<tr>
<td>assessment</td>
<td>Finding out about what has happened and what needs to be done.</td>
</tr>
<tr>
<td>authorised</td>
<td>Allowed; given permission; given the okay.</td>
</tr>
<tr>
<td>breach</td>
<td>The act of breaking a law or agreement.</td>
</tr>
<tr>
<td>data</td>
<td>Stored information.</td>
</tr>
<tr>
<td>Codes of Practice</td>
<td>Rules created by the Privacy Commissioner to regulate how certain industries deal with personal information. These codes form part of the Privacy Act.</td>
</tr>
<tr>
<td>consequences</td>
<td>What will happen as the result of an action.</td>
</tr>
<tr>
<td>contain</td>
<td>Hold in; prevent (an event) from happening or (effects) from spreading. For example, you could contain a data breach by closing down a website.</td>
</tr>
<tr>
<td>disclose</td>
<td>Tell (to another person or agency).</td>
</tr>
<tr>
<td>employee</td>
<td>A person who is employed or contracted by an agency.</td>
</tr>
<tr>
<td>enquiries</td>
<td>Questions or queries.</td>
</tr>
<tr>
<td>grounds</td>
<td>Good (legal) reasons.</td>
</tr>
<tr>
<td>Health Industry Privacy Code (HIPC)</td>
<td>The privacy laws that apply to the health industry.</td>
</tr>
<tr>
<td>incident</td>
<td>A thing that has happened.</td>
</tr>
<tr>
<td>individual(s)</td>
<td>A person or people.</td>
</tr>
<tr>
<td>interference</td>
<td>A breach of one or more of privacy principles 1-5 or 8-12 and an adverse consequence; or a breach of principles 6 or 7.</td>
</tr>
<tr>
<td>Word</td>
<td>What it means in this workbook</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------</td>
</tr>
<tr>
<td>investigate</td>
<td>Find out what is happening or has happened.</td>
</tr>
<tr>
<td>jurisdiction</td>
<td>The power and authority to carry out an investigation.</td>
</tr>
<tr>
<td>mandatory</td>
<td>Must be done; is required to be done, e.g., by law.</td>
</tr>
<tr>
<td>mitigate</td>
<td>Reduce, contain or lessen risk or harm.</td>
</tr>
<tr>
<td>notification</td>
<td>Telling other people or the authorities.</td>
</tr>
<tr>
<td>notify</td>
<td>Tell.</td>
</tr>
<tr>
<td>obligation</td>
<td>Requirement.</td>
</tr>
<tr>
<td>occur</td>
<td>Happen.</td>
</tr>
<tr>
<td>practice</td>
<td>The usual way of doing something.</td>
</tr>
<tr>
<td>procedural provisions</td>
<td>What needs to be done, and how.</td>
</tr>
<tr>
<td>purpose</td>
<td>The reason for doing something.</td>
</tr>
<tr>
<td>retain</td>
<td>Keep.</td>
</tr>
<tr>
<td>retention</td>
<td>Keeping or holding on to.</td>
</tr>
<tr>
<td>sensitive</td>
<td>High risk; could be harmful to people or the organisation.</td>
</tr>
<tr>
<td>significance</td>
<td>Importance.</td>
</tr>
<tr>
<td>simultaneously</td>
<td>At the same time.</td>
</tr>
<tr>
<td>source</td>
<td>Where something comes from.</td>
</tr>
<tr>
<td>succession</td>
<td>One after the other.</td>
</tr>
<tr>
<td>third party</td>
<td>Another person or agency (i.e. not you or the person directly concerned).</td>
</tr>
<tr>
<td>transferred</td>
<td>Sent somewhere else.</td>
</tr>
<tr>
<td>unauthorised</td>
<td>Not allowed.</td>
</tr>
<tr>
<td>voluntary</td>
<td>Optional; open to choice.</td>
</tr>
</tbody>
</table>
Additional resources

Icebreakers and training ideas: http://www.businessballs.com/
Tribunal decisions: www.nzlii.org

How to contact the Office of the Privacy Commissioner

Website: www.privacy.org.nz

PO Box 10-094
The Terrace, Wellington 6143
Fax: (04) 474 7595

Enquiries line (for general enquiries):
0800 803 909 (from 8.30am to 5pm, Monday to Friday)
enquiries@privacy.org.nz

04-474 7590 (Wellington)
09-302 8680 (Auckland)
Appendix

The HIPC rules: quick reference guide

Rule 1 - purpose for collection
Health information must only be collected when:
- the collection is for a lawful purpose
- the purpose is connected with the functions of the agency, and
- it is necessary to collect the information for that purpose

Rule 2 - source of information
Health information must usually be collected from the person who the information relates to. But the Code does allow you to collect information from other people in limited cases, for instance, when:
- the person concerned authorises collection from someone else
- obtaining it from the person concerned would undermine the purpose of the collection
- this is necessary in order for a public sector body to uphold or enforce the law
- this is necessary for the purposes of court or tribunal proceedings

Rule 3 - what to tell an individual
When an agency directly collects health information, it has to take reasonable steps to make sure that person concerned knows things like:
- why it is being collected
- who will see the information
- whether the person is required to give the information or whether it is voluntary, and
- what will happen if the information isn’t provided

Again, there are sometimes good reasons for not letting a person know. For example, it could undermine the purpose of the collection, or it is just not possible to tell the person.

Rule 4 - manner of collection
Health information must not be collected by unlawful means or by means that, in the circumstances, are unfair or unreasonably intrusive.
Rule 5 - storage and security

It is impossible to prevent all mistakes. But health agencies must ensure that they take reasonable steps to prevent the loss, misuse or disclosure of health information.

Rule 6 - access

People have the right to ask for access to personal information about themselves.

Agencies can refuse to give access in some limited situations, for instance, where giving the information would:

- endanger a person’s safety
- prevent the detection and investigation of criminal offences, or
- involve an unwarranted breach of someone else’s privacy

Rule 7 - correction

People have a right to ask an agency to correct information about themselves if they think the information is wrong.

If the agency does not want to correct the information, it does not usually have to. But if it does not correct the information, it must give the person the opportunity to add their views about what the correct information is.

Rule 8 - accuracy

Before using health information, an agency must take reasonable steps to ensure it is:

- accurate
- up-to-date
- complete
- relevant
- not misleading

Rule 9 - retention

Agencies must not keep health information for too long. They can only keep it for as long as is necessary for any lawful purpose of use.

Rule 10 - use

Agencies must use health information for the same purposes for which they obtained that information.

Other uses are occasionally permitted (for example, where this is necessary to enforce the law, or where the use is directly related to the purpose for which the agency obtained the information).
Rule 11 - disclosure

Unless another law overrides the HIPC, health agencies must not disclose personal information unless an exception applies. An agency can disclose information if it reasonably believes, for example, that:

- disclosure is one of the purposes for which the agency obtained the information
- disclosure is necessary to uphold or enforce the law
- disclosure is necessary for court or tribunal proceedings
- the person concerned authorised the disclosure, or
- the information is going to be used in a form that does not identify the person concerned

Rule 12 - unique identifiers

Some agencies give people a unique identifier instead of using their name. Examples are a driver’s licence number, a student ID number or an IRD number.

An agency cannot use the unique identifier given to a person by another agency. People are not required to disclose their unique identifier unless this is one of the purposes for which the unique identifier was set up (or directly related to those purposes).

An important exception in the health context is the National Health Index Number (the NHI Number). The NHI number is a unique identifier which can be widely assigned and used (see rule 12(3) and schedule 2 of the HIPC).