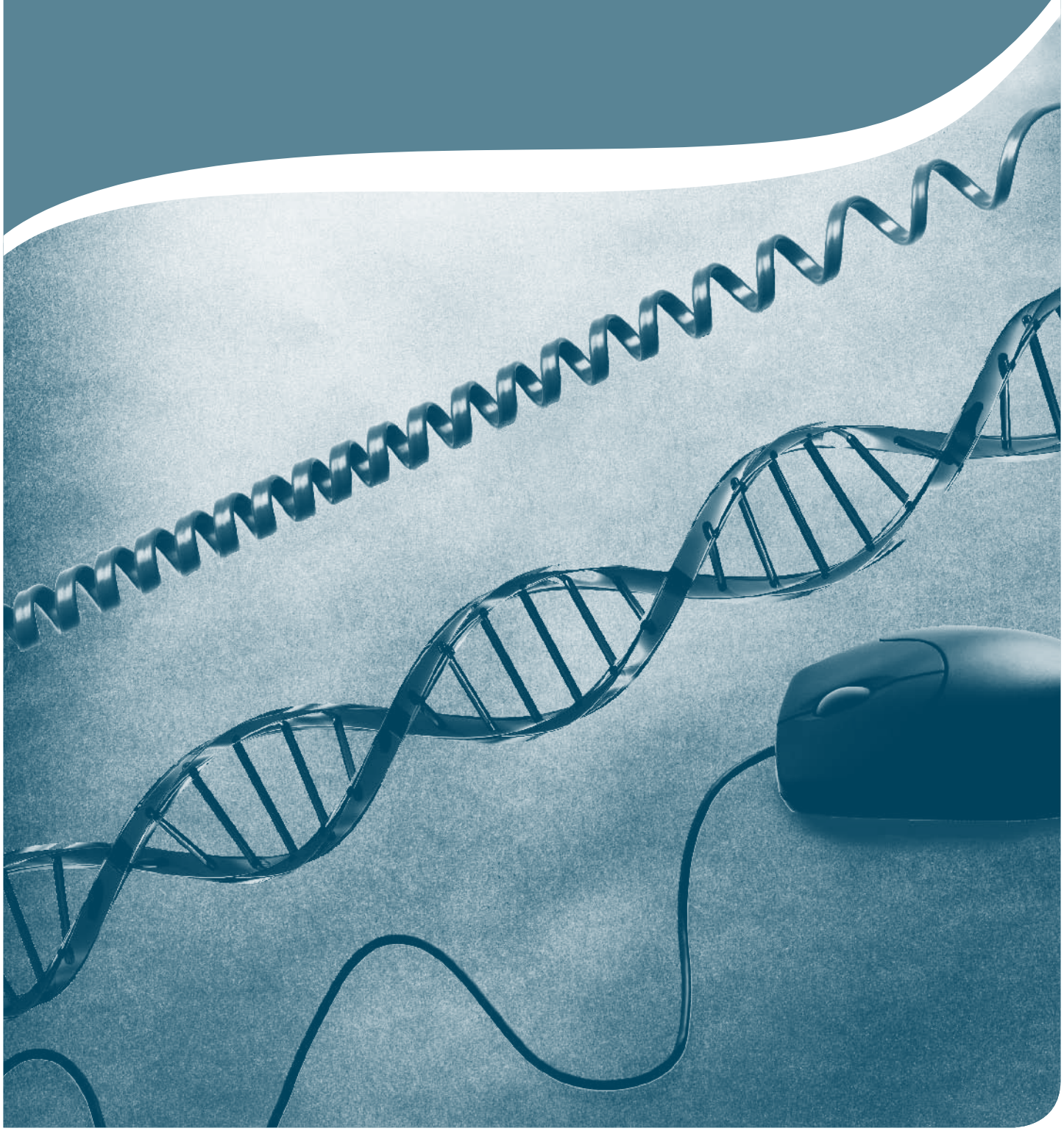
Privacy Commissioner
Te Mana Matapono Matatapu

Health Information Privacy Code 1994

Incorporating amendments and including revised commentary



New edition December 2008

Incorporating amendments:

Amendment No 1 (Temporary) – now spent

Amendment No 2 – commenced 30 July 1995

Amendment No 3 – commenced 30 September 1998

Amendment No 4 – commenced 10 April 2000

Amendment No 5 – commenced 30 July 2000

Amendment No 6 – commenced 1 November 2007

The introduction, commentary, notes and appendix are not part of code

The Health Information Privacy Code 1994 comprises clauses 1-7 and rules 1-12.

The notes and commentary contain references to statutory provisions, explanation, practical illustrations and other useful information. The commentary is not binding and does not form part of the code. Always refer to the rules or clauses.

Sometimes the commentary refers to, or paraphrases, provisions from the Privacy Act or other enactments. We suggest that you refer to the enactments themselves rather than relying on paraphrases. Many of the sections from statutes referred to will be found in the appendix.

In accordance with the Acts & Regulations Publication Act 1989, changes have been made to the layout and formatting of the code and other enactments. These changes do not modify the effect of the law.

Contents

HEALTH INFORMATION PRIVACY CODE 1994

Foreword

Nearly every interaction with an agency generates information. Mostly that information will be trivial (though even trivial data can reveal a surprising amount about the person to whom it relates). When it comes to *health* information, though, there is little we would consider to be trivial. Because of this, we are used to information about our health being treated in particular ways.

We expect it to be considered as **confidential**, because in all likelihood it was collected in a situation of confidence and trust. We want it to be treated as **sensitive**, because it may include details about our body, lifestyle, emotions and behaviour. And we accept that a piece of information may have **ongoing use** if it becomes clinically relevant in the future, long after it was initially collected.

This code of practice recognises those expectations that health information should be treated differently. It applies specific *rules* to agencies in the health sector to better ensure the protection of individual privacy. With respect to health information collected, used, held and disclosed by health agencies, the code substitutes for the information privacy *principles* in the Privacy Act.

The rules in the code might be summarised as follows:

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

Put like that, the rules can be seen for what they are – a straightforward and sensible blueprint for the management of people's information. There are, of course, many important complexities that need to be understood; the rules themselves should always be studied carefully before attempting to apply them.

These rules are enforceable by complaining to my office, and then, if necessary, to the Human Rights Review Tribunal. There may be financial and other consequences for agencies that breach the rules, so it is important that they are studied and complied with by those working in the health sector.

I consulted many individuals and groups when preparing and amending this code and commentary and am grateful for the many helpful comments made to me. I welcome further comments on the code, including suggestions for change, at any time.

Marie Shroff

Privacy Commissioner

Introduction

This edition of the code includes an updated version of the commentary published in previous editions. This commentary is not part of the code and is not binding. It is provided to assist understanding. When assessing how best to comply with the law, reference should always be made to the wording of the code itself.

The code applies to health information relating to identifiable individuals. This means that while it covers, for example, information about an individual's medical and treatment history, disabilities or accidents, contact with any health or disability service providers and information about donations of blood or organs, it does not apply to anonymous or aggregated statistical information where individuals cannot be identified.

The code applies to all agencies providing personal or public health or disability services from the largest hospitals through to sole health practitioners. It covers, for example, primary health organisations, district health boards, rest homes, supported accommodation, doctors, nurses, dentists, pharmacists and optometrists. It also applies to some agencies that do not provide health services to individuals but that are part of the health sector, such as ACC, the Ministry of Health, the Health Research Council, health insurers and professional disciplinary bodies.

Health agencies and individual practitioners will need to ensure that their internal operational procedures comply with the code, for instance in the design of computer systems and the use of forms and internal procedures relating to the collection, use and disclosure of health information. Staff briefing or training will be an essential element of operational procedures. Compliance with privacy obligations is an integral part of good information handling procedures, and is closely linked to good clinical practice.

A number of health agencies and practitioners subject to this code must also comply with the Code of Health and Disability Services Consumers' Rights and their own professional ethical obligations. In many cases these ethical requirements may be even more stringent than the legal obligations imposed by this code.

The principles of informed choice and consent relating to autonomy, responsibility and accountability should also be borne in mind in the provision of health and disability services. Those principles accord with many of those expressed in this code. However, there is an important distinction between the need to obtain informed consent and the obligation for health agencies to be open about the purpose for which they collect and hold health information.

Guidance on that code and matters of informed consent can be obtained from the Health and Disability Commissioner's office.

References

Throughout the code there are cross references to other parts of the code and other laws and publications. A number of the sections in statutes referred to are set out in the appendix.

The Office of the Privacy Commissioner has a number of other publications available touching upon privacy issues in the health and disability sectors. Contact the office or visit the website at **www.privacy.org.nz** to see what is currently available. Publications include:

- Compilations of materials from the Office of the Privacy Commissioner on health information and privacy;
- *On the Record: A Practical Guide to Health Information Privacy,* 1999;
- *Health Information Check-up brochure,* 2007.

It may be useful to refer to specialised publications on the Privacy Act such as:

- Dr Paul Roth, *Privacy Law and Practice,* LexisNexis, looseleaf service.

Privacy Officers, legal advisers and others who wish to consider in detail the access and correction provisions (ie. rules 6, 7 and Parts 4 and 5 of the Privacy Act), may find Eagles, Taggart, Liddell, *Freedom of Information in New Zealand,* OUP, Auckland, 1992 useful.

Other publications of interest include:

- Skegg and Paterson (ed), *Medical Law in New Zealand,* 2007;
- Te Puni Kokiri, *Privacy of Health Information: Te Matatuakiri me te Matatapu O Nga Korero Hauora,* 1994;
- Mental Health Commission, *Protecting Your Health Information: A Guide to Privacy Issues for Users of Mental Health Services,* 1999.

Preliminary

1 TITLE

This code of practice may be referred to as the Health Information Privacy Code 1994.

2 COMMENCEMENT

This code is to come into force on 30 July 1994.

Note: *Clause 2(2) was revoked, and clause 2(1) accordingly renumbered as clause 2, by Amendment No 5.*

COMMENTARY

Section 53 of the Privacy Act sets out the two main legal effects of a code of practice such as this one. First, any "action" (which also includes policies or practices) that would otherwise breach an information privacy principle is deemed not to breach that principle if done in accordance with the code. Secondly, failure to comply with the code, even if not otherwise a breach of a principle, is deemed to be a breach of a principle.

This means that the code has the effect of law on all health agencies that are holding, using or disclosing health information.

See Part 6 of the Privacy Act.

3 INTERPRETATION

In this code,—

commencement, in relation to this code, means the coming into force of the code

disability services includes goods, services, and facilities—

(a) provided to people with disabilities for their care or support or to promote their inclusion and participation in society or independence; or

(b) provided for purposes related or incidental to the care or support of people with disabilities or to the promotion of the inclusion and participation in society, and independence of such people

ethics committee means—

(a) the Ethics Committee of the Health Research Council of New Zealand or an ethics committee approved by that committee; or

(b) the National Advisory Committee on Health and Disability Support Services Ethics; or

(c) an ethics committee constituted in accordance with the currently applicable Operational Standard for Ethics Committees promulgated by the Ministry of Health; or

(d) an ethics committee established by, or pursuant to, any enactment

health agency means an agency referred to in clause 4(2) and, for the purposes of rules 5 to 11, is to be taken to include,—

(a) where an agency holds health information obtained in the course of providing health or disability services but no longer provides such services, that agency; and

(b) with respect to any health information held by a health agency (being a natural person) at the time of the person's death, his or her personal representative

health information means information to which this code applies under clause 4(1)

health practitioner has the meaning given to it by section 5(1) of the Health Practitioners Competence Assurance Act 2003

health professional body means an authority empowered to exercise registration and disciplinary powers under the Health Practitioners Competence Assurance Act 2003

health services means personal health services and public health services

health training institution means a school, faculty, or department referred to in paragraph 4(2)(d)

personal health services means goods, services, and facilities provided to an individual for the purpose of improving or protecting the health of that individual, whether or not they are also provided for another purpose; and includes goods, services, and facilities provided for related or incidental purposes

principal caregiver, in relation to any individual, means the friend of the individual or the member of the individual's family group or whānau who is most evidently and directly concerned with the oversight of the individual's care and welfare

public health services means goods, services, and facilities provided for the purpose of improving, promoting, or protecting public health or preventing population-wide disease, disability, or injury; and includes—

(a) regulatory functions relating to health or disability matters; and

(b) health protection and health promotion services; and

(c) goods, services, and facilities provided for related or incidental functions or purposes

representative, in relation to an individual, means,—

(a) where that individual is dead, that individual's personal representative; or

(b) where the individual is under the age of 16 years, that individual's parent or guardian; or

(c) where the individual, not being an individual referred to in paragraphs (a) or (b), is unable to give his or her consent or authority, or exercise his or her rights, a person appearing to be lawfully acting on the individual's behalf or in his or her interests

rule means a rule set out in clause 5.

the Act means the Privacy Act 1993

Note: *Clause 3 was amended by Amendment No 2 (affecting definitions of health professional body, health registration enactment, and registered health professional) and Amendment No 4 (affecting the definition of hospital). Amendment No 5 revoked clause 3(2) and accordingly renumbered clause 3(1) as clause 3. Amendment No 6 removed definitions of hospital, health registration enactment, and registered health professional. It also added definitions of personal health services, public health services, and health practitioner, as well as modifying the definitions of ethics committee and disability services.*

COMMENTARY

"Disability services", "personal health services" and "public health services" are defined in the same way as in the New Zealand Public Health and Disability Act 2000.

"Ethics committee": see commentary to rule 2.

"Health agency" and "health information": see commentary to clause 4.

Health practitioner: not every health professional is a "health practitioner". If an individual provides health services, even where the particular discipline is not listed in the Health Practitioners Competence Assurance Act 2003, that individual will still be a "health agency". However, the code uses the term "health practitioner" to refer to those specific professionals for whom Parliament has established a registration and discipline regime. Extra discretions to disclose information are permitted for health practitioners in rule 11, based on additional controls placed on them by their statutory registration and discipline regime. If a health practitioner acts unethically or

negligently there are statutory discipline mechanisms and sanctions administered by a "health professional body".

Alternative and complementary practitioners, while they are likely to be health *agencies,* will only be considered "health practitioners" if their discipline is listed in the Health Practitioners Competence Assurance Act.

"Principal caregiver" is defined in the same way as in the Mental Health (Compulsory Assessment and Treatment) Act 1992.

"Representative": The definition mirrors the one in section 22B of the Health Act 1956:

- Paragraph (a) refers to a "personal representative". This is a legal term referring to the deceased person's executor or administrator.
- Paragraph (b) applies regardless of any custody or access arrangements. A non-custodial parent or guardian will still be a representative for the purposes of the code.
- Paragraph (c) would include:
  - welfare guardians 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 (subject to the terms of that power of attorney);
  - a person who is clearly acting in the best interests of a patient that cannot speak for themselves through mental or physical incapacity (for instance an able-bodied friend presenting with an incapacitated accident victim).

The code uses the term "representative" only occasionally – mainly to provide extra privacy protection in circumstances where the individual is unable to exercise his or her own rights. It is also relevant to section 22F of the Health Act 1956, which gives an individual's representative the ability to obtain information about that individual. Paragraph (c) encompasses both formal statutory relationships such as those listed above and emergency situations where an individual is incapacitated, or incompetent to provide authorisation, and no formal statutory relationship exists. However, a person appearing to be acting contrary to the interests of the individual would not be regarded as an individual's representative under paragraph (c).

A lawyer for a child appointed by a court under section 7 of the Care of Children Act 2004 would probably not be a representative (since paragraph (c) excludes the deceased and children under 16 from its application) but would be able to exercise privacy rights on behalf of the child as his or her agent.

The code is to be interpreted in accordance with normal rules of statutory interpretation and is subject to the Interpretation Act 1999. Accordingly, a word or expression used in the code has the same meaning as in the Act under which it was issued.

Where other legislation refers to a principle of Privacy Act, in relation to health information or a health agency it can generally be taken as referring to the equivalent rule in this code.

Terms and expressions defined in the Privacy Act and used in this code include: action; agency; collect; Commissioner; correct; document; individual; individual concerned; information privacy request; news activity; news medium; publicly available information; unique identifier; and working day. Definitions of these terms may be found in the appendix.

See Privacy Act, section 2; New Zealand Public Health and Disability Act 2000, section 2; Health Act 1956 section 22B; Health and Disability Commissioner Act 1994, sections 2 and 4; Health Practitioners Competence Assurance Act 2003, section 2; Mental Health (Compulsory Assessment and Treatment) Act 1992, section 2; Interpretation Act 1999; Care of Children Act 2004.

4 APPLICATION OF CODE

(1) This code applies to the following information or classes of information about an identifiable individual:

(a) information about the health of that individual, including his or her medical history; or

(b) information about any disabilities that individual has, or has had; or

(c) information about any health services or disability services that are being provided, or have been provided, to that individual; or

(d) information provided by that individual in connection with the donation, by that individual, of any body part or any bodily substance of that individual or derived from the testing or examination of any body part, or any bodily substance of that individual; or

(e) information about that individual which is collected before or in the course of, and incidental to, the provision of any health service or disability service to that individual.

(2) This code applies in relation to the following agencies or classes of agency:

Health and disability service providers

(a) an agency which provides health or disability services; or

(b) within a larger agency, a division or administrative unit (including an individual) which provides health or disability services to employees of the agency or some other limited class of persons; or

(c) a person who is approved as a counsellor for the purposes of the Injury Prevention, Rehabilitation, and Compensation Act 2001; or

Training, registration, and discipline of health professionals, etc

(d) a school, faculty or department of a tertiary educational institution which provides the training or a component of the training necessary for the registration of a health practitioner; or

(e) an agency having statutory responsibility for the registration of any health practitioners; or

(f) a health professional body; or

(g) persons appointed or designated under the Health and Disability Commissioner Act 1994; or

Health insurance, etc

(h) Revoked

(i) an agency which provides health, disability, accident, or medical insurance, or which provides claims management services in relation to such insurance, but only in respect of providing that insurance or those services; or

(j) an accredited employer under the Injury Prevention, Rehabilitation, and Compensation Act 2001; or

Other

(k) an agency which provides services in respect of health information, including an agency which provides those services under an agreement with another agency; or

(l) a district inspector, deputy district inspector, or official visitor appointed pursuant to section 94 of the Mental Health (Compulsory Assessment and Treatment) Act 1992; or

(la) a district inspector or deputy district inspector appointed pursuant to section 144 of the Intellectual Disability (Compulsory Care and Rehabilitation) Act 2003; or

(m) an agency which manufactures, sells, or supplies medicines, medical devices, or related products; or

(n) an agency which provides health and disability services consumer advocacy services; or

(o) the department responsible for the administration of the Coroners Act 2006, but only in respect of information contained in documents referred to in section 29(1) of that Act; or

(p) the agencies specified in Schedule 1.

Note: *Clause 4(2) was substituted by Amendment No 5. Clause 4(2)(c) and (d), (e), (j), and (o) were amended, clause 4(2)(h) was revoked and clause 4(2)(la) was added by Amendment No 6.*

COMMENTARY

The code applies only to health information about identifiable individuals. Health information, as defined in the code, includes disability information (for instance, information collected as part of a needs assessment process). Incidental information obtained in connection with the provision of health services and that identifies the individual is also covered. The code does not apply to employee information. However, the health sector must comply with the provisions of the Privacy Act as it relates to employee information. Employees may exercise their rights, for instance to seek access to their personnel records, under the relevant parts of the Privacy Act.

Clause 4(1) is derived from section 22B of the Health Act but extends the scope of paragraph (d) and adds paragraph (e).

The main agencies to which this code applies are those providing health or disability services such as health professionals, hospitals, ambulance services and rest homes. Also covered are agencies that no longer provide health services, but still hold information from the time when they did.

The positions of agencies, their employees and agents are governed by sections 3, 4 and 126 of the Privacy Act (which are set out in the appendix). A health agency is responsible for the actions of those working for it, whether paid or unpaid, except where the person concerned was clearly acting outside his or her authority or instructions. Health agencies need to train their workers in their responsibilities under the code – it is possible that both agency and worker will be liable for an interference with privacy.

Generally the code will continue to apply to health information even when it is transferred out of the country. For the purposes of rules 5, 8, 9, 10 and 11, information transferred out of New Zealand is still considered to be held by the agency. Similarly, for the purposes of rules 6 and 7, information held by an agency includes information held outside New Zealand by that agency. However, any action required by overseas law is not considered a breach of the code.

ELECTRONIC HEALTH INFORMATION

The code, like the Privacy Act, is technology neutral. As such, it deals with health information in the same way in whatever form it is held. However, there are specific considerations that should be borne in mind when considering the security of health information stored in electronic form. Some of these considerations are addressed in the commentary to rule 5.

Clause 3 defines the terms: health or disability services; health agency; health information; health services; and health practitioner. Refer also to section 10 of the Privacy Act.

2: Health information privacy rules

5 HEALTH INFORMATION PRIVACY RULES

The information privacy principles are modified in accordance with the Act by the following rules which apply to health information and health agencies:

Rule 1: PURPOSE OF COLLECTION OF HEALTH INFORMATION

Health information must not be collected by any health agency unless—

(a) the information is collected for a lawful purpose connected with a function or activity of the health agency; and

(b) the collection of the information is necessary for that purpose.

Note: *An action is not in breach of this rule if it is authorised or required by or under law: Privacy Act 1993, section 7(4).*

COMMENTARY

Rules 1, 2, 3 and 4 deal with key aspects of collection including the purpose of collection (rule 1), the source of the information (rule 2), transparency towards the individual (rule 3) and manner of collection (rule 4).

Health agencies sometimes receive information about patients volunteered to them by third parties such as family members. The definition of "collection" in section 2 of the Privacy Act provides that passively receiving unsolicited information is not a collection for the purposes of rules 1 to 4, regardless of whether the information is received in person or by way of a letter, email, or telephone call.

However, although clarifying the volunteered information may not turn the health agency from recipient to collector, a conscious act such as taking the opportunity to ask for more or unrelated information is likely to amount to a collection that is subject to rules 1 to 4.

In any case, once the information has been obtained and is held, it is subject to the other rules in the code regardless of how it was received.

Rule 1 requires agencies to consider the information they need to carry out their functions. This rule helps to refine and streamline information collection procedures. Collecting information that is not necessary for the present or reasonably anticipated purposes of the agency is prohibited by the rule. Agencies should keep their information collection practices, such as the design and use of databases and standard forms, under review so that the information collected is useful, relevant, and not excessive.

2: Health information privacy rules

LAWFUL PURPOSE

Agencies may only collect information for lawful purposes. A purpose does *not* require explicit legal authority before it is lawful, though statutory bodies should ensure that they are legally empowered to perform the function or activity.

All agencies should consider whether their purpose for collecting information is:

- prohibited or regulated by law; and/or
- within their legal powers.

If the law makes no mention of a particular purpose for collection it is likely to be lawful.

PURPOSES CONNECTED WITH FUNCTION OR ACTIVITY OF AGENCY

Most of the agencies covered by the code provide health services. As such, the central purpose for collection will be to provide care and treatment, in other words:

Care and treatment

To record the individual's health status and the care or treatment given and to assist in the further care or treatment of that individual or, in cases where a communicable disease is diagnosed, the care and treatment of other individuals.

However, there are also likely to be other, related, purposes, such as:

Administration

To assist in the administrative aspects of care-giving or treatment such as billing, claims management and financial audit to detect and prevent fraud, and utilisation reviews to assist in service planning and development to meet statutory reporting obligations. Administrative information may well be collected or stored separately from medical information but it is closely related to episodes of care and treatment.

Training and education

To act as a record of the health care problem and its management so as to assist in developing and maintaining expertise and competence by those involved in the treatment and management of that patient, or the future treatment and management of other patients in similar circumstances.

Monitoring

To monitor the quality of patient care, treatment and health status.

While there may be other "directly related" purposes, these are some of the usual purposes for a health services provider. Disability service providers, funders, ACC and the various other types of agencies covered by the code will have quite different purposes, as may particular health service providers.

Rule 1 provides the only restriction on the purposes for which an agency may collect health information in the code. It effectively obliges health agencies to be clear about how and why they intend to use the information they collect, *before* the point of

2: Health information privacy rules

collection, if possible. This requirement should not be unduly onerous, as the scope of legitimate purposes for collecting health information can be very broad. Later, in rule 3, this clarity of purpose is linked to an obligation to be open about this purpose with the individual concerned.

NECESSITY FOR PURPOSE

Health information should only be collected if it is actually required for the lawful purposes or functions undertaken.

While a wide range of information relating to an individual's health, lifestyle, behaviour and habits might be collected for care and treatment purposes, in most cases only part of that information is likely to be available for use for administrative purposes (the *use* of information is constrained by rule 10).

Health funders generally have no need to collect the same depth and breadth of health information about identifiable individuals as do providers for care and treatment purposes, although they may need statistical or aggregated information. Any collection of health information about identifiable individuals by an agency should be demonstrably related to its activities.

Also, District Health Board employees relying on section 22C(2)(j) of the Health Act 1956 to collect information are expected to seek identifiable patient information only with the individual's consent or where the identifying information is "essential".

Health researchers will be expected to justify their purpose in collecting personal information in a formal way when seeking ethical approval for research projects. Research protocols should specify the personal information to be collected and explain why the collection of the information is necessary for the purpose.

See rules 2, 3 and 4.

Rule 2: SOURCE OF HEALTH INFORMATION

(1) Where a health agency collects health information, the health agency must collect the information directly from the individual concerned.

(2) It is not necessary for a health agency to comply with subrule (1) if the agency believes, on reasonable grounds, that—

(a) the individual concerned authorises collection of the information from someone else having been made aware of the matters set out in rule 3(1); or

(b) the individual is unable to give his or her authority and the health agency, having made the individual's representative aware of the matters set out in rule 3(1), collects the information from the representative or the representative authorises collection from someone else; or

(c) compliance would—

(i) prejudice the interests of the individual concerned; or

(ii) prejudice the purposes of collection; or

(iii) prejudice the safety of any individual; or

(d) compliance is not reasonably practicable in the circumstances of the particular case; or

(e) the collection is for the purpose of assembling a family or genetic history of an individual and is collected directly from that individual; or

(f) the information is publicly available information; or

(g) the information—

(i) will not be used in a form in which the individual concerned is identified; or

(ii) will be used for statistical purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(iii) will be used for research purposes (for which approval by an ethics committee, if required, has been given) and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(h) non-compliance is necessary—

(i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) for the protection of the public revenue; or

(iii) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

2: Health information privacy rules

(i) the collection is in accordance with an authority granted under section 54 of the Act.

Note: *An action is not in breach of this rule if it is authorised or required by or under law: Privacy Act 1993, section 7(4).*

COMMENTARY

Rule 2 is intended to reinforce individual autonomy and people's control over their health information. Individuals are best able to control the flow of their health information when it is collected directly from them; they can choose whether, what and how much to provide. Rule 3 ensures that individuals are properly informed when details of their personal health information are solicited from them. However, there are a number of reasons why health agencies might not be able, or wish, to collect information directly from the individual. Rule 2 contains exceptions to the general rule.

ETHNICITY OR ETHNIC GROUP

Self-identification should be the means of collecting information about ethnicity, rather than identification by an observer. Agencies should regularly review whether they need to collect such information (rule 1). If it *is* collected, care must be taken to explain the reasons for doing so to the individual (rule 3), and to ensure the information is safeguarded (rule 5) and only used and disclosed for the correct purpose and to the correct people (rules 8, 10 and 11).

PEOPLE WITH DISABILITIES

Rule 2 helps address concerns about how some agencies deal with some people with disabilities. The concerns relates to the assumption – often unfounded – that an agency needs to go beyond an individual with a disability to a third party to obtain personal information. Such assumptions can undermine privacy and personal autonomy. It is insulting for a person with a disability to be ignored while questions concerning him or her are directed to someone else.

EXCEPTIONS TO RULE 2

There are a number of exceptions to rule 2, and examples of some of these have been provided below. If an agency in a particular case relies on an exception to a rule, it must be able to justify its actions. The onus of proving the exception is on the relevant health agency: Privacy Act, section 87. Health agencies should carefully consider any departures from the rules and, where appropriate, suitably document their reasons.

Whenever information is collected from a source other than the individual concerned, it is important to verify the information as soon as possible with the individual (where practicable). This will assist in complying with rule 8.

(a) Individual authorises collection from someone else

The individual concerned may expressly authorise collection from someone else. Given the importance of health and disability service consumers' personal autonomy and the general sensitivity of health information, seeking an authorisation is nearly always to be preferred to relying on some other exception to rule 2. In seeking authorisation, the agency should make the individual aware of relevant matters under rule 3(1) such as purpose for collection, intended recipients and any consequences for not supplying the information. In this way, personal privacy and autonomy are upheld to the greatest extent possible, while still allowing the flexibility of collection from another source.

(b) Representative authorises collection from someone else

Sometimes the individual will be unable to provide authorisation (where unconscious, for example). In those circumstances, exception (b) permits collection of information from the representative or from a third party with the representative's authority. Where authorisation to collect elsewhere is sought from an individual or his or her representative, the agency is expected to make the individual or representative aware of the matters required by rule 3(1).

(c) Compliance prejudices individual's interests, purpose of collection or individual safety

Sometimes, collecting necessary health information from a person in an acute state with a mental illness might compromise his or her care and treatment. In such cases the required health information might have to be collected from another person who is in a better position to supply it, in order to ensure proper treatment can be provided. Similarly, in emergencies it might prejudice the individual's interests, or even their safety, to delay matters by seeking to collect information only from the individual.

The accuracy of any health information collected from others should be verified with the individual at a later time where practicable.

(d) Compliance is not reasonably practicable

This exception may apply where the individual is not able to provide the information needed, such as when he or she is unconscious or is not competent to provide the information. For example, a person with a significant intellectual disability or an acute mental illness may be unable to understand what is being asked of them or to offer accurate answers.

In some situations, individuals will be unable to supply health information because they do not have the information or technical knowledge or skill to supply it. For example, where an individual gives a doctor a blood sample for testing, a laboratory derives the health information from the sample. Even if the individual did know his or her blood group, it is likely that the doctor would seek this information from a laboratory because of the serious risk to treatment of inaccurate information. Exceptions (a) and (e) may also apply.

2: Health information privacy rules

Similarly, ACC requires health information to process claims and to facilitate rehabilitation. Some of this health information will be collected from individual claimants but much is obtained from health and disability service providers on the basis of the individual's authorisation and its own statutory powers under the Injury Prevention, Rehabilitation and Compensation Act 2001.

It may not be practicable to collect information directly from very young children. In that case, the parents or guardians of the child (as representatives) should be asked to authorise collection from another source. Only if that course of action is not practicable should the agency rely on exception (d).

(f) Publicly available information

Publicly available means information contained in a book, newspaper or other publication that is, or will be, generally available to members of the public. It includes information in a public register, for example, the births register (see Privacy Act, section 2).

Information on a website or other internet resource is also publicly available if it is able to be freely accessed by the public.

(g)(iii) Research purposes

The exception applies to research whether or not it is the type that requires ethical approval. If ethical approval is required, then the exception applies only if such approval is obtained.

The requirement to obtain ethical approval arises independently of this code under other laws, professional ethics or funding requirements. For example, researchers seeking funding from the Health Research Council will need ethics committee approval when research involves the use of personal information:

- from medical or other private or confidential files;
- which may personally identify a research participant;
- for which the participant has not given consent for the purposes of the research which is proposed;
- which is considered to be sensitive or valuable in a personal, social, cultural or commercial sense.

(Health Research Council, *Guidelines on Ethics in Health Research,* 2005)

Researchers seeking ethical approval should set out in the research protocol if they intend to depart from rule 2(1) and their reasons, whether ethical, practical or scientific, for doing so. Where the researcher proposes to collect information from someone else, then this should be with the authority of the individual concerned except in special circumstances. For instance, the researcher may intend to collect personal information from someone else, without the authority of the individual concerned, because that individual is untraceable, incapacitated, or for some other good reason. If so, this approach would need to be explained in the protocol to be approved by an ethics committee, and then carried out in accordance with any conditions the committee specifies.

Researchers may wish to use health records without the individual's authorisation. This may be for scientific, practical or ethical reasons. If ethics committee approval is being sought, these reasons should be explained.

The potential benefits of the research may also need to be explained to the ethics committee and may be weighed against the loss of privacy.

See Blair Stewart, "Medical Research and the Privacy Act" 1/3 *Human Rights Law and Practice,* December 1995, 141-177. See also Health Research Council, *Guidelines on Ethics in Health Research* (2005), Part 6, "Health Research and Privacy: Guidance Notes for Health Researchers and Ethics Committees" (also printed in 1/4 *Human Rights Law and Practice,* March 1996, 196-210), and the currently applicable Ministry of Health operational guidelines for ethics committees.

(h) Conduct of proceedings

One example of where this exception might be applicable is when a patient seeks a review of a compulsory assessment order, a community treatment order or an inpatient order and the health agency involved in treating him or her under the Mental Health (Compulsory Assessment and Treatment) Act 1992 collects information from other people.

(i) Privacy Commissioner authorises collection

The specific authorisation power in section 54 is not intended for any routine collection but rather for special circumstances. Note also that the power cannot be exercised when the individual concerned has specifically refused to authorise the collection. Section 54 is set out in the appendix.

IDENTIFICATION OF SOURCE

Clearly identifying the source of the information in records (which might include the name of the person supplying the information and the time or date) will assist in complying with rule 2 and rule 8.

See rules 1, 3 and 4.

2:

Health information privacy rules

Rule 3: COLLECTION OF HEALTH INFORMATION FROM INDIVIDUAL

(1) Where a health agency collects health information directly from the individual concerned, or from the individual's representative, the health agency must take such steps as are, in the circumstances, reasonable to ensure that the individual concerned (and the representative if collection is from the representative) is aware of—

(a) the fact that the information is being collected; and

(b) the purpose for which the information is being collected; and

(c) the intended recipients of the information; and

(d) the name and address of—

(i) the health agency that is collecting the information; and

(ii) the agency that will hold the information; and

(e) whether or not the supply of the information is voluntary or mandatory and if mandatory, the particular law under which it is required; and

(f) the consequences (if any) for that individual if all or any part of the requested information is not provided; and

(g) the rights of access to, and correction of, health information provided by rules 6 and 7.

(2) The steps referred to in subrule (1) must be taken before the information is collected or, if that is not practicable, as soon as practicable after it is collected.

(3) A health agency is not required to take the steps referred to in subrule (1) in relation to the collection of information from an individual, or the individual's representative, if that agency has taken those steps in relation to the collection, from that individual or that representative, of the same information or information of the same kind for the same or a related purpose, on a recent previous occasion.

(4) It is not necessary for a health agency to comply with subrule (1) if the agency believes on reasonable grounds, that—

(a) Revoked

(b) compliance would—

(i) prejudice the interests of the individual concerned; or

(ii) prejudice the purposes of collection; or

(c) compliance is not reasonably practicable in the circumstances of the particular case; or

(d) non-compliance is necessary to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences.

Note: *An action is not a breach of this rule if it is authorised or required by or under law: Privacy Act 1993, section 7(4). Rule 3(4)(a) was revoked by Amendment No 4.*

COMMENTARY

Rule 3, like rule 2, is intended to reinforce individual autonomy and people's control over their health information by requiring transparency of collection. When people know what is intended to happen with their health information they can make an informed choice about what they reveal, and place limits on further use or disclosure.

REQUIREMENT TO INFORM THE INDIVIDUAL

Consistent with the notions of autonomy and control, individuals need to be made aware of a number of things when information is collected from them. Set out in rule 3(1), these things include:

(a) Fact of collection

In most cases in the health sector the fact of collection will be obvious from the context. However, that is not always the case. For instance, patients might be treated behind a one-way screen while other professionals listen in. In other cases, agencies might make a visual or audio recording in psychiatric care and treatment. In such cases the individual would not necessarily be aware that information is being collected unless they were told.

Some additional restrictions may apply to the collection of information about people in compulsory care. Section 68 of the Mental Health (Compulsory Assessment and Treatment) Act 1992 restricts the making of video and audio recordings of patients under compulsory care without consent, as does section 52 of the Intellectual Disability (Compulsory Care and Rehabilitation) Act 2003.

(b) Purpose of collection

The collection of health information for care and treatment and the related routine administrative aspects are usually clear and may require only brief explanation. However, it will not always be apparent where agencies collect health information for training or research, or for incidental purposes like chaplaincy services. If so, the agency should make the individual aware of such purposes.

Openness about purpose can assist health agencies to use and disclose the information in the future. Rules 10 and 11 always allow information to be used and disclosed for a particular purpose where doing so was one of the reasons for obtaining the information in the first place. The collecting agency should have communicated the purposes to the individual at the point of collection in accordance with rule 3. When they understand the purpose of collection and the proposed uses and disclosures, individuals can decide whether they wish to provide information, by weighing up the benefits of doing so against the consequences of not providing the information.

2:

Health information privacy rules

One advantage of complying with rule 3 is that individuals will be prepared for a use or disclosure, which might otherwise come as a surprise to them. Another advantage is that it can help establish that the use or disclosure was an intended purpose in the event that a complaint is made.

(c) Intended recipients of information

The individual will not always be aware of the intended recipients of the information, particularly where health information is sought for training, research and monitoring purposes, or to meet administrative or funder requirements.

Some accident and medical centres send consultation information to an individual's general practitioner after the individual has received treatment at the centre, as do specialists. While this is good medical practice, it should be done only with the individual's knowledge since he or she may not otherwise anticipate the disclosure.

Similarly, if a clinical test result is to be stored on a regional or national results repository it is important that the individual is made aware of this before undergoing the test.

(d) Agency details

Individuals need this information so they can exercise their rights of access.

(e) Voluntary or mandatory, legal authority

Individuals are entitled to know whether they are obliged to supply information. Sometimes only some of the information collected on a form will be mandatory. The form should be designed so that people can clearly see what is, or is not, required of them. Where information is required under law, individuals must be made aware of which law makes the supply mandatory. Agencies should give sufficient detail to enable people to check their legal position if they wish.

(f) Consequences of not supplying information

Agencies should not coerce information from individuals. The right to refuse to provide information that is not required by law must be respected.

However, consequences may legitimately result from an individual's failure or refusal to provide information. Those consequences need to have been properly communicated by the agency beforehand. The consequences of not supplying information might include, for example, that:

- a particular treatment cannot effectively be continued;
- the individual might not be eligible for a subsidy; or
- a claim cannot be granted or processed.

In addition to the other obligations under rule 3, where a researcher is collecting information directly from an individual, the individual should be informed that the provision of information is voluntary and that refusal to provide all or any part of the requested information will not affect the current or future provision of health care to the individual in any way.

(g) Rights of access and correction

These are set out in rules 6 and 7.

RELATIONSHIP TO INFORMED CONSENT

Providing this explanation to individuals will help them to decide what information (if any) to make available to the health agency. It may also help agencies to comply with requirements to obtain informed consent to treatment.

However, informed consent to treatment and compliance with rule 3 are *not* interchangeable. Compliance with rule 3 will not necessarily ensure consent to treatment is informed for the purposes of the Code of Health and Disability Services Consumers' Rights. Neither will compliance with provisions of that code necessarily ensure compliance with rule 3.

REQUIREMENT TO INFORM REPRESENTATIVE

It is not always possible to collect information directly from the individual. For instance, an individual may be unconscious or may not be competent because of their age or disability. In such circumstances, if health agencies collect information from the representative, they should give the representative the explanations that would otherwise have been given to the individual.

Where individuals have diminished competence, health agencies should still give them an explanation at the level of their understanding. This is particularly important when dealing with children who may lack legal capacity to consent to treatment but who nevertheless have sufficient competency to absorb a rule 3 explanation and to have an opinion about the use and disclosure of their health information.

REASONABLE STEPS TO INFORM

Rule 3 requires that agencies take reasonable steps to inform the individual about what is to be done with his or her information. These might include:

- an oral explanation in appropriate language;
- a notice on display in the health agency's premises;
- an explanatory letter;
- an explanatory note on standard printed or electronic forms used for capturing health information; or
- explanatory brochures.

Agencies should also consider how best to overcome barriers to understanding that may exist due to:

- culture or language;
- age;
- physical disability (eg. impaired hearing);

2: Health information privacy rules

- mental disability;
- physical or mental state or confusion; or
- reading difficulties.

Agencies may need to give a more detailed explanation when particularly intimate or sensitive information is sought or where it plans to use the information in an unexpected way.

In some circumstances there may be a legal obligation to provide an interpreter when explaining things to a person who speaks another language or who, for instance, is unable to understand spoken English because of physical disability (see Mental Health (Compulsory Assessment and Treatment) Act 1992, section 6; Code of Health and Disability Services Consumers' Rights, Right 5).

Sometimes the individual may wish to have a friend or family member present if being given oral explanations. Under the Code of Health and Disability Services Consumers' Rights a consumer is entitled to have one or more support persons of his or her choice present, except where safety may be compromised or another consumer's rights may be unreasonably infringed.

LAYERED PRIVACY NOTICES

Complex information flows can be difficult to convey concisely and accurately, particularly in the limited time available to most clinical consultations. It may be helpful for medium and large health agencies to consider preparing a layered privacy notice, to help communicate effectively about how they handle health information. Layered notices can concisely summarise key information in the first 'layer', then provide more detailed information in the second layer. This accomplishes the goal of informing patients in general terms about the likely movements of their information, while also directing them to a source of more detailed explanation should they want or need it.

When creating a layered privacy notice, the first layer can be thought of as the 'highlights' of the privacy notice. It should give an overview of how the agency handles health information, use clear and straightforward language and provide the most important information first. Agencies may link to more detailed information, either by a reference (eg. "a copy of the full privacy policy is available on our website at …") or by a direct electronic link.

The second layer is the full privacy policy, whether broken up by topics into selected units or listed in full. The format especially lends itself to websites, but a similar approach is possible through innovative linking of posters, brochures and detailed written policies.

One way to easily get the benefit of a layered privacy notice is to simply summarise, simplify and provide links to the full privacy policy. However, before doing this it may be wise to review the current policy to ensure that it accurately reflects how the agency currently handles personal information.

See the Office of the Privacy Commissioner's "Questions and Answers about Layered Privacy Notices", www.privacy.org.nz/effective-website-privacy-notices

TIMING

Rule 3 requires that agencies should inform the individual about the collection of their information either before the information is collected or as soon as practicable after the collection. For example, at an appropriate time after an unconscious patient regains consciousness or a previously disordered patient is able to comprehend, he or she should be informed about any information about them that has been collected from another source.

Sometimes it will not be practicable for the collecting agency to provide explanations later (eg. an ambulance officer may have no further dealings with the individual).

REPEAT EXPLANATIONS

If individuals have regular dealings with a health agency, they will need a full explanation the first time information is collected but not necessarily on every subsequent occasion, provided the information and the purposes for which it will be used remain the same. Whether further steps are required may depend on how recently an explanation was given, the importance or sensitivity of the information and the individual's circumstances. For example, someone with memory loss may not recall the initial explanation and need the explanation to be repeated. Unless the agency collecting the information is reasonably sure that the individual is aware of rule 3 matters (perhaps because the individual is attending a follow-up consultation with the same professional) the agency should notify the individual whenever new or additional information is collected. This requirement should not be onerous. When brochures are available that explain in a generic way why information is being collected, it may be sufficient to draw these to an individual's attention on subsequent occasions.

CHAPLAINCY

Before the Privacy Act, many hospitals routinely asked for individuals' religious affiliation without explaining why or who would see the details. The Privacy Act requires greater openness. The information was often given to chaplains or staff who visited patients. Sometimes, lists of names were released outside the hospital to religious organisations.

2: Health information privacy rules

Hospitals can set reasonable policies that allow them to collect information about an individual's religious affiliations for the purpose of passing it to a hospital chaplain or an outside spiritual adviser. Hospitals doing so need to explain the purpose of collection and the intended recipients in accordance with rule 3. Some hospitals have chosen not to ask individuals about religious affiliation, but instead ask whether they would like a chaplain to see them or to have their own spiritual adviser informed. This is more consistent with notions of individual autonomy than former practices. Hospitals might also ask about dietary requirements – including religious-based requirements.

GENETIC INFORMATION

Genetic information, and the use of information obtained from genetic tests, raises some important issues. Information obtained from a genetic test on an individual relates not only to the individual undergoing the test, but also to his or her relatives.

When carrying out a genetic test on behalf of an individual, agencies should carefully consider whether they have fulfilled their obligations under rule 3. This is of particular concern if a positive result for the condition being tested for would have implications for the health of the individual's relatives. Agencies should have clearly communicated policies on what they will do where they receive information that may be vital to an individual's relatives' health.

EXCEPTIONS TO THE RULE

There are a number of exceptions to rule 3. For instance, non-compliance is permitted under rule 3(4) where:

(b) Compliance is prejudicial to purposes of collection

For example, an agency might not disclose the fact that information was being collected behind a one-way screen if knowledge of the fact may disrupt the process and compromise care and treatment, as long as the collection was taking place for proper medical reasons.

(c) Compliance not reasonably practicable

Compliance may not be practicable for example, where an individual is unconscious, or in cases of emergency where giving a full explanation at the time may delay matters to the serious detriment of the individual. Collection of health information by ambulance staff in an emergency would sometimes fall within this exception (or exception 3(4)(b)(i)).

See rules 1, 2 and 4. See also Ministry of Health, *Consent in Child and Youth Health: Information for Practitioners,* 1998, and Code of Health and Disability Services Consumers' Rights ("Right to be fully informed" and "Right to support").

2: Health information privacy rules

Rule 4: MANNER OF COLLECTION OF HEALTH INFORMATION

Health information must not be collected by a health agency—

(a) by unlawful means; or

(b) by means that, in the circumstances of the case,—

(i) are unfair; or

(ii) intrude to an unreasonable extent upon the personal affairs of the individual concerned.

Note: *An action is not a breach of this rule if it is authorised or required by or under law: Privacy Act 1993, section 7(4).*

COMMENTARY

This rule is not limited to collection of information directly from an individual.

UNLAWFUL MEANS

Health agencies must ensure that measures used to collect information comply with any applicable laws. Collection by unlawful means may include, for example, collection by means that breach of the Mental Health (Compulsory Assessment and Treatment) Act or the Fair Trading Act, bribing officials to corruptly release information (see Crimes Act 1961, sections 105, 105A and 105B), or using listening devices to intercept private communications (which is a "crime against personal privacy" under section 216B of the Crimes Act 1961). If officials act outside their lawful powers to collect information, this might amount to collection by unlawful means.

UNFAIR MEANS

Unfair means of collection could include, for example, deliberately misstating the purpose of collection to the individual concerned, videoing or taping an individual without consent, adopting an overbearing or threatening manner, exaggerating the consequences of not supplying information or creating an impression that supply is mandatory when it is not. Unfair means in relation to collections from sources other than the individual concerned might include, for instance, misrepresenting who is requesting the information or why it is needed.

UNREASONABLE INTRUSION

Although the Health Information Privacy Code is generally concerned with information privacy rather than physical privacy, rule 4 may require consideration of physical privacy issues as well. There may be an unreasonable intrusion into privacy if, for

2: Health information privacy rules

instance, information is collected in a setting that allows other people to overhear the collection. In considering what is unreasonable intrusion, agencies may need to pay attention to:

- **Physical privacy**, especially when sensitive or intimate information is collected. While it may be reasonable to expect an individual to provide their full name in a GP's reception area, it would be unreasonable to collect more sensitive information in a public area where the individual might be overheard. Where practical, the use of printed forms to collect sensitive information is preferable.
- **Streamlining the collection process** so that intimate questions are not repeatedly asked of the same individual in a short space of time.
- Ensuring that people who collect health information have **training in privacy issues**. It is also important that staff who deal with sensitive information do not become desensitised to the importance of the information to the individual concerned.
- **Others present** – some individuals may wish members of their whānau or family to be present (or excluded) when particular information is being collected. The presence (or absence) of particular staff may also be an issue when some sensitive topics are discussed.
- Identity of the **person collecting information** (eg. role, personal relationship, seniority, etc) – sometimes individuals may prefer to give information to someone with whom they have developed a relationship than to other staff members.
- Particular concerns or **preferences expressed by the individual**. For example, respecting the individual's wish not to have a consultation in the presence of medical students.
- **Cultural sensitivities** of the individual concerned – this may relate to the nature of the information collected as well as the form and context in which it is sought and the person to whom it is given.

Be aware also that the Code of Health and Disability Services Consumers' Rights requires consumers to be treated with respect by health agencies, and that services should be provided in a way that respects the dignity and independence of the individual. Right 1(2) of that Code provides that consumers have the right to have their privacy respected in the provision of health and disability services.

While all health information is sensitive, some categories of information are particularly so. Assessment of whether a means of collection is unreasonably intrusive may depend on the context and the sensitivity of the information. For example, particularly sensitive information could include information relating to:

- sexual life (eg. sexual orientation, sexual practice, fertility, past pregnancies or terminations, births outside marriage, sterilisation, contraception, STDs, and sexual dysfunction);
- ethnicity;

- HIV status;
- diseases or conditions carrying social stigma;
- mental health history;
- life expectancy; or
- addiction.

Sometimes information is sensitive because, if it were disclosed, it could be used to discriminate against the individual.

Taking steps to enhance and preserve privacy is also desirable when disclosing information (such as test results) to the individual concerned.

HEALTH RESEARCH

Inducements that could be regarded as constituting undue influence should not be offered to research participants to provide information. Any reward for participation in health research (monetary or otherwise) should be approved by an ethics committee. Researchers who are in positions of power over individuals should not use their position to influence the decisions of individuals to provide personal information for research purposes.

See also rules 1, 2 and 3. See also the right to be treated with respect and the right to dignity and independence in the Code of Health and Disability Services Consumers' Rights.

2:

Health information privacy rules

Rule 5: STORAGE AND SECURITY OF HEALTH INFORMATION

(1) A health agency that holds health information must ensure that—

(a) the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against:

(i) loss; or

(ii) access, use, modification, or disclosure, except with the authority of the agency; or

(iii) other misuse; and

(b) if it is necessary for the information to be given to a person in connection with the provision of a service to the health agency, including any storing, processing, or destruction of the information, everything reasonably within the power of the health agency is done to prevent unauthorised use or unauthorised disclosure of the information; and

(c) where a document containing health information is not to be kept, the document is disposed of in a manner that preserves the privacy of the individual.

(2) This rule applies to health information obtained before or after the commencement of this code.

Note: *An action is not a breach of this rule if it is authorised or required by or under law: Privacy Act 1993, section 7(4).*

COMMENTARY

The following points are intended as discussion notes about various aspects of information security and should not be regarded as a complete or definitive treatment of this extensive and continually evolving subject.

Medium-sized and large-sized agencies should have business, human resource and security policies, and business continuity plans that address these issues.

Small agencies should keep asking themselves the question, "What could go wrong?" and "How can we improve the business process to avoid or reduce the risk of something going wrong?"

PHYSICAL SECURITY

Appropriate arrangements are needed to protect the physical security of health information while in use and storage. Suitable arrangements might include:

- physically securing, and restricting access to, the areas in which health information is stored;
- taking simple precautions in respect of paper records and digital media, such as locking filing cabinets, locking unattended rooms etc;
- taking precautions to protect paper records and computer data stores from fire, deterioration and other hazards;
- requiring all access keys, cards, passwords etc to computer systems or networks to be physically secure or subject to defined and enforced security procedures;
- controlling access to areas where fax machines are located;
- positioning computer screens used for entering or manipulating health information so that they cannot be seen by unauthorised personnel; and
- using screen saver programs and security screens so computer screens cannot be seen by unauthorised personnel.

OPERATIONAL SECURITY (USERS)

Appropriate arrangements are needed to protect the operational security of health information. Suitable procedures might include:

- requiring as part of an employment contract or contract of service that all persons collecting, using or disclosing health information comply with this code and ensuring their responsibilities relating to health information privacy and access are clearly outlined;
- withholding, as far as practicable, access to health information from equipment installers or maintenance staff;
- making records anonymous for health education purposes and using fictitious information when training individuals in the use of systems;
- requiring people making entries on health records to sign or otherwise record their names on those entries, with the addition of automatic "footprinting" in electronic records;
- keeping health information, whether paper records, computer disks or tapes, on the agency's premises where possible;
- where staff are authorised to take health information off the premises, requiring it to be kept securely (for example in a locked file or case);
- avoiding collecting health information in public waiting areas where discussions can be overheard. Discussions involving health information should be conducted where they cannot be overheard by members of the public or unauthorised personnel;
- arranging appropriate staff training and supervision – steps taken such as training to challenge unrecognised and unaccompanied visitors, will also help to control theft and promote staff and patient safety;

2:

Health information privacy rules

- maintaining formal procedures for employees who are leaving the agency including reclaiming identity badges, passes and keys, and cancelling passwords and logins; and
- effective implementation and monitoring of agency security and privacy policies.

OPERATIONAL SECURITY (COMPUTER SYSTEMS)

When considering the operational security of computer systems, consider:

- maintaining a list of personnel who are authorised to use the system;
- changing passwords at frequent intervals;
- developing rules on levels of access and taking steps to ensure that access to different categories of information is available only to authorised users;
- implementing an audit mechanism to detect unauthorised access and ensuring regular checks are made of the audit mechanism;
- ensuring all staff receive appropriate training on privacy and security policies and the proper use of the computer – including policies against browsing personal files for any purpose unrelated to that staff member's job;
- establishing disciplinary procedures for staff who access information without authorisation; and
- using strong passwords and anti-theft hardware and software on laptops.

Health research projects should use anonymising techniques such as (at minimum):

- removing names from the records; and
- using an identifier to ensure that individuals can be identified only by reference to a cross index.

TECHNICAL SECURITY

Some considerations are most effectively addressed when selecting and implementing computer systems. Suitable procedures might include:

- validating software used for recording, processing, storing and retrieving health information through detailed audit, and certifying software as suitable for the uses to which it is put;
- providing for, as far as possible, the validation of all data entered on systems to ensure their accuracy;
- adopting procedures to ensure data cannot be passed between computers or discrete systems within the same computer without authority;
- setting up system security, anti-virus, and anti-spyware update procedures;
- taking reasonable steps before a computer interface is established, with a system to ensure the arrangement does not increase the risk of unauthorised access;
- ensuring that a business continuity plan is developed, tested and regularly re-assessed; and

- where mobile devices are used to interface with an electronic health system, ensuring that information stored on the devices is 'synced' with a central system for archival and security purposes.

SECURITY OF TRANSMISSION

Publish guidelines to all staff for the use of mail, faxes and email for transmitting health information. Guidelines might include:

Facsimile

When appropriately used, and subject to appropriate security safeguards, fax transmission can provide a quick and satisfactory means of communication.

Problems arise if information is transmitted to the wrong number through misdialling or staff changes at the receiving agency. Faxes are also often received at unattended machines.

Consider:

- locating fax machines out of public areas, with controlled access;
- restricting the use of fax machines to authorised staff and ensuring that there is secure delivery to intended clinical staff;
- using programmed numbers to avoid misdialling;
- regularly checking the accuracy of pre-programmed numbers;
- producing and distributing an official and regularly updated list of fax numbers assigned to commonly used locations (with a clear expiry date for each edition) to ensure that fax numbers are current and accurate;
- controlling the type of information that may be sent by fax;
- requiring staff to telephone the intended recipient before transmission to ensure the information can be uplifted immediately;
- carefully checking fax confirmation reports to ensure correct transmission (and to enable rapid action in the case of incorrect transmission);
- retaining fax activity history reports to check unauthorised transmissions etc; and
- using unique identifiers, rather than names, to ensure transmission of confidential information about identifiable individuals does not occur. Carefully controlled, this severance of personal information also permits the faxing of documents, but care is needed to ensure that different documents do not become mixed.

Email

Email poses special problems in privacy. Use of email to transmit health information may result in the information being stored on several hard drives, not all of which may be secure from unauthorised access. There is also a risk of interception during the transmission, as email commonly passes through a number of computers on the way to its final destination.

2: Health information privacy rules

Some agencies may, for such reasons, entirely avoid its use. Others may use it only for less sensitive purposes, such as arranging appointments. An email security policy for a health agency might include:

- establishing guidelines on the nature of information which may be transmitted by email;
- encryption and virtual private networks;
- enforcing security of access;
- using addresses received electronically where possible to minimise the risk of key-entry errors where information is sent to the wrong person;
- using addresses based upon roles rather than people's names;
- producing and distributing an official and regularly updated list of email addresses (with a clear expiry date for each edition) to ensure that the addresses are current and accurate; and
- discouraging the inclusion of lengthy 'chains' of responses in emails, as sensitive information may be unwittingly included in an early response.

Post

The type of ordinary physical delivery (eg. general post, registered post, couriered post, track-and-trace, hand delivered post) should be appropriate to the nature of the records.

When sending health information by post:

- ensure that postal items safely enter the postal system before they can be intercepted by third parties. Steps might include a locked posting box for outgoing mail and keeping incoming and outgoing mail out of public areas;
- care must be taken not to display health information on the outside of envelopes. Consider double-enveloping, for example if a return address should not be displayed;
- postcards should not generally be used;
- medical records should not normally be given to third parties to pass onto patients unless this is authorised by the individual concerned or their representative; and
- information on digital media (CDs, memory sticks or similar) should be encrypted.

DISPOSAL OR DESTRUCTION OF HEALTH INFORMATION

Health information that is no longer required either by the individual concerned or the health agency (including retiring practitioners) must be transferred or destroyed in a manner that ensures its confidentiality.

TRANSFER

Records may be transferred (in a manner that preserves privacy) to:

- the individual or designated agent. Consideration may be given to offering individuals the choice of having their records transferred to them or disposed of in accordance with their wishes. For instance, some Māori may wish to have special procedures adopted for passing records to their whānau after death;
- another appropriate agency to provide further services (eg. a GP); or
- an appropriate statutory or professional body to hold as a custodian (eg. Archives New Zealand under the Public Records Act 2005).

DESTRUCTION

If destruction is proposed, the requirements of the Health (Retention of Health Information) Regulations 1996 (see Appendix) must be met. The Public Records Act 2005 is also relevant for public sector health agencies such as District Health Boards and hospitals.

Physical records may be destroyed by controlled incineration, ensuring that individual records are not lost or removed during the process and that the resulting waste does not include fragments of readable personal information. Tearing up patient records (including print-outs of computer-held patient information) and disposing with normal waste is an inadequate means of disposal.

Computerised records – including computer hard disks, floppy disks, CDs, DVDs and photocopy machine hard disks – may be rendered unreadable through the use of an appropriate physical or electronic process. Simple deletion of a magnetic disk is inadequate since facilities exist that can recover all or part of the data. Advice on specific techniques can be found in NZ ICT Security Manual, or NZSIT 402, available from the Government Communications Security Bureau website www.gcsb.govt.nz.

Be aware that physical destruction of the storage medium is the only way to be absolutely sure that information cannot be recovered from a hard drive. In most cases this will not be necessary, but consideration should be given to destroying, where appropriate, the hard drives of old computers and photocopiers that are being disposed of.

Health information held by individual health practitioners (or agencies who are natural persons) retiring from practice may still be required for lawful purposes. Retiring practitioners should take proper steps to ensure that relevant records are left with another competent practitioner, the individuals concerned, or an appropriate statutory or professional body.

2: Health information privacy rules

SECURITY PLAN

Every medium and large health agency should undertake the systematic development of a suitable security plan with associated policies and procedures.

This would normally commence by carrying out a project to classify all the information held by the agency, to help it understand the extent and sensitivity of its information asset base. An information risk assessment can then be undertaken to determine the possible risk factors associated with the loss, access, use, modification, disclosure or misuse of personal information and other data assets, and the possible outcomes that will result from such loss, access etc.

The information classification scheme and the information risk assessment should consider all classes of information (eg. personal, staff, business, statistical etc) and all media (eg. paper, computer, disks, USB Flash ROM 'memory sticks' and external hard drives, X-ray images, other network terminals and facilities etc), which the information may be recorded or transmitted upon.

Completion of the information classification system and risk assessment exercise will place the agency in an excellent position to develop an appropriate security plan and appropriate policies and procedures. A good plan will provide for the whole process to be reviewed regularly and modified in the light of experience, evolution of the agencies data assets and new discoveries in the risk assessment.

Guidance on the objectives of information security is given by ISO standards AS/NZS ISO/IEC 17799:2006 and AS/NZS ISO/IEC 27001:2006.

Agencies in the government sector may also be required to comply with: *Security in the Government Sector*, Department of Prime Minister and Cabinet and NZ SIT 401/402, Government Communications Security Bureau.

Generally these documents offer guidance and set minimum standards. To establish reasonable safeguards may well require better standards than the minimum, especially as technology often evolves faster than standards can be updated.

PRIVACY BREACH DISCLOSURE

A health information privacy breach occurs when there is any breach of the 12 health information privacy rules. Privacy breaches often involve people's health information being accidentally lost or disclosed, for instance by being faxed or emailed to the wrong person. Another common risk is the loss of a laptop, memory stick or other electronic storage device, either on its own or as a by-product of another mishap for instance, when a laptop is left in a car that is stolen.

It is vital that health agencies consider how to deal with privacy breaches ahead of time and develop an appropriate policy.

There are four key steps to consider when developing such a policy, and when responding to a breach or suspected breach:

1 **Breach containment and preliminary assessment**. Immediate steps should be taken to contain the breach and stop further loss or disclosure of health information. A suitable person should be chosen to lead the investigation, and a team assembled to assist him or her if necessary. Any people who urgently need to know of the breach, whether internal or external, should be informed.

2 **Evaluation of the risks associated with the breach.** Establish the sensitivity of the lost or accidentally disclosed health information and any context that may make some or all of the information more sensitive than normal. Was the information encrypted or anonymised? How did the breach occur? Who is affected by it? Could any other harm result from the breach?

3 **Notification.** Are there particular risks that would be incurred by not notifying the individuals concerned such as identity theft, financial loss, physical harm or significant humiliation? If so, it will probably be appropriate to carry out a direct notification, providing information about the incident and its timing, as well as a description of the health information involved in the breach and what the agency has done to control or to reduce the harm. Depending on the level of risk identified in step two, it may then be appropriate to notify external agencies such as insurers, professional bodies, the Office of the Privacy Commissioner and the Police.

4 **Prevention.** Security, by its nature, can never be absolute. However, it is likely that a thorough investigation of a breach will reveal ways in which procedures can be improved to decrease the likelihood of future mishaps, particularly if the breach was systemic rather than an isolated occurrence. A prevention plan should be developed, possibly including a physical and technical security audit and a review of employee training, policies and procedures.

A privacy breach checklist can be obtained from the Privacy Commissioner's website www.privacy.org.nz.

See rules 6, 7, 9 and 11 and the Health (Retention of Health Information) Regulations 1996. See also Office of the Privacy Commissioner, *Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist,* 2007. Public sector agencies should consider the Public Records Act 2005 and any General Disposal Authorities issued by the Chief Archivist. Also refer to OECD, *Guidelines for the Security of Information Systems and Networks, 2002* and AS/NZS ISO/IEC 17799:2001 Information Technology: Code of Practice for Information Security Management. ISO/IEC 17799 *Information Security Management,* NZ Health Information Service, *Information Systems Security and Data Protection,* 1993. Please also refer to other New Zealand Standards such as chapters 14 and 15 of NZS 8153:2002 *Health Records* and NZS HB 8169:2002 *Health Network Code of Practice.*

2: Health information privacy rules

Rule 6: ACCESS TO PERSONAL HEALTH INFORMATION

(1) Where a health agency holds health information in such a way that it can readily be retrieved, the individual concerned is entitled—

(a) to obtain from the agency confirmation of whether or not the agency holds such health information; and

(b) to have access to that health information.

(2) Where, in accordance with subrule (1)(b), an individual is given access to health information, the individual must be advised that, under rule 7, the individual may request correction of that information.

(3) The application of this rule is subject to—

(a) Part 4 of the Act (which sets out reasons for withholding information); and

(b) Part 5 of the Act (which sets out procedural provisions relating to access to information); and

(c) clause 6 (which concerns charges).

(4) This rule applies to health information obtained before or after the commencement of this code.

Note: *This rule is subject to provisions in enactments which authorise or require personal information to be made available or Acts which prohibit, restrict, or regulate the availability of personal information: Privacy Act 1993, section 7(1) and (2). Under section 7(3) it is also subject to certain regulations which prohibit, restrict, or regulate the availability of personal information.*

COMMENTARY

Under rule 6 individuals have a right to access information held about themselves by a health agency. The right is subject to limited reasons for refusing a request, which are set out in section 27 to 29 of the Privacy Act and are reprinted in the appendix.

The right is to have access to *information.* The rule does not determine ownership of documents. Rule 6 does not give individuals the right to take away original records, although access to originals may of course be sought and granted. A request may not be refused on the basis that the agency 'owns' the records or that they are not the requester's property. Nor may an agency refuse a request on the basis that money is owed to it by the requester.

Parts 4 and 5 of the Privacy Act, referred to throughout this material, are set out in the appendix.

ACCESS PROVISIONS

Reasons for refusing access to health information are covered by Part 4 (sections 27 to 29) of the Privacy Act.

Procedural provisions relating to access to health information are covered by Part 5 (sections 33 to 45) of the Privacy Act. These provisions apply to requests:

- to obtain confirmation of whether or not an agency holds health information;
- to be given access to health information; and
- for correction of health information.

Requests may be made orally or in writing. They need not refer to the Privacy Act or be in any special format. However, individuals seeking access may receive a faster response to requests if they clearly define the information they want.

Certain information is exempted from access requests by section 55 of the Privacy Act. For instance, rule 6 does not apply to information contained in any correspondence or communication between the Privacy Commissioner and an agency relating to an investigation. There is a similar exemption for information relating to investigations by the Ombudsmen.

The following is a general commentary on the requirements of the Privacy Act in relation to the health sector and requests for confirmation and access. Not every applicable section is referred to and a detailed understanding of the requirements can only be obtained by referring directly to the Act.

Note that requests by individuals or their representatives under section 22F of the Health Act are required, in some respects, to be treated as if they were access requests under rule 6 – see rule 11(4) and the associated commentary.

More detailed guidance on these requirements is given in texts on the Privacy Act and the Official Information Act 1982, such as:

Privacy Law and Practice;
Freedom of Information in New Zealand.

IDENTITY OF PERSON SEEKING ACCESS (SECTION 45)

Where a request for access is made, an agency must:

- satisfy itself as to the identity of the individual making the request. This may involve requiring identification where the individual is not known personally;
- ensure the information sought is received only by that individual or his or her agent. This may involve using registered mail or requiring that the individual sign a receipt for the information; and

- ensure that where a request is made by an agent, the agent has a current written authority or is otherwise properly authorised to obtain the information. Agencies should set out their own policies for what evidence of authorisation will be acceptable and communicate those policies to staff.

Access under rule 6 is only for the individual or his or her agent. Representatives who have not been authorised as an individual's agent for a particular request may ask for disclosure under rule 11 or seek access in accordance with section 22F of the Health Act (read together with rule 11(4)(b)). See 'Subrule 4: Requests under section 22F of the Health Act', on page 67 for further explanation of these provisions.

ACCESS RIGHTS OF CHILDREN

All individuals, including children, have the right of access to their own health information although a young child may not have the ability to make his or her own request. When a child does make a request, the agency is obliged to treat that request in accordance with the provisions of the Privacy Act and this code (although note, as mentioned below, that access might be refused in a case of an individual under the age of 16 where the disclosure of the information would be contrary to that individual's interests – section 29(1)(d) Privacy Act).

A child or young person will on occasion ask some other person, usually an adult, to obtain access to that child's health records. Sometimes that might be the lawyer for the child or it could be a parent or guardian. As with any other request for access, health agencies are obliged under section 45 of the Privacy Act to take reasonable precautions to ensure that the person making the request is properly authorised to obtain the information.

Section 22F of the Health Act, read together with rule 11(4)(b), entitles a child's representative (their parent or guardian) to request access to their child's health information. This might be done in connection with the provision of health services to the child, such as a routine request for health records to be transferred from one GP to another when the family moves home. Under section 22F(4), the Privacy Commissioner can investigate a refusal to act on a representative's request. Rule 11(4)(b) of the code allows, but does not require, the refusal of a request where the child either does not want the disclosure to occur or where the disclosure would not be in the child's interests. See 'Subrule 4: Requests under section 22F of the Health Act', on page 67.

There will be many circumstances where health information about children and young people may quite properly be disclosed to parents and guardians under rule 11 (rather than rule 6).

URGENT REQUESTS (SECTION 37)

Urgent requests should be dealt with as soon as reasonably possible. If an individual wants a request to be treated as urgent, he or she must explain why. Agencies need to develop appropriate processes to accommodate urgent requests when they are received.

AGENCY TO GIVE ASSISTANCE (SECTION 38)

Agencies have a duty to give reasonable assistance to an individual making a request so that the request meets the requirements of the Privacy Act or, if necessary, to direct the request to the appropriate agency. A health agency is required to provide this assistance whether or not it holds the information sought.

It is good practice, as well as a legal obligation, to treat every access request with care and attention. For instance, if an oral request is received it is sensible to clarify with the requester exactly what they are seeking and to help him or her put the request into writing. Keeping the requester updated with progress in responding to their complaint, if it is complex, can also be reassuring to them and will hopefully lessen the risk of a complaint being made to the Privacy Commissioner.

TRANSFER OF REQUESTS (SECTION 39)

Where information:

- is not held by a health agency but is believed to be held by another agency; or
- is held by a health agency but believed to be more closely connected to the functions or activities of another agency,

the agency receiving the request is required to transfer the request promptly, and in any case within 10 working days, and to inform the individual accordingly.

Transferring a request is a useful (and underused) way of dealing with a request for information that was originally received from another agency. If a transfer is necessary it will generally be appreciated by individuals if this is done promptly and the individual kept informed about what has been done.

While there is no obligation to obtain the individual's permission *before* transferring their request, it may be wise to consider whether the individual should be contacted first if the request is for particularly complex or sensitive information. This will help avoid the requester being alarmed by the transfer to another agency, if he or she was not expecting it.

2: Health information privacy rules

DECISIONS ON REQUESTS (SECTION 40)

Decisions on requests must be made as soon as reasonably practicable and not later than 20 working days after the receipt of the request. In that time the health agency must:

- decide whether the request is to be granted;
- decide what form to release the information in (refer also sections 42 and 43); and
- notify the individual of this accordingly.

Health agencies should have in place appropriate procedures so that time limits are met. "Working day" is defined in section 2 of the Privacy Act and excludes Saturdays and Sundays, national statutory holidays and the period from 25 December to 15 January.

Requests do not necessarily have to be dealt with immediately, but agencies must have procedures that allow requests to be dealt with as soon as reasonably practicable and within 20 working days. They should also have procedures to allow requests to be dealt with on a more urgent basis if requested. However, even an urgent request does not require an *instant* response. Health agencies should always have sufficient time to consider how best to respond to an access request.

EXTENSION OF TIME LIMITS (SECTION 41)

The time limits in respect of decisions may be extended if:

- the request is for a large quantity of information; or
- consultations are necessary to make a decision on the request, so that a response cannot be made within the original time limit.

Where the time limits have been extended the individual must be informed of the:

- period of extension;
- reason for extension; and
- right to make a complaint to the Privacy Commissioner about the extension.

REASONS FOR REFUSING ACCESS (SECTIONS 27-28)

A list of the only reasons for refusal allowed in the Privacy Act is set out in sections 27 to 29 (part 4 – see the appendix for a complete list). However, section 7(2)(a) of the Privacy Act also allows for withholding of information if a provision in another statute imposes a prohibition or restriction in relation to the availability of personal information. This means that an obligation of confidentiality imposed by a statute (as opposed to, say, the general ethical obligation of clinical confidentiality) will take precedence over the rule 6 right of access.

If information is to be withheld by a health agency it can be done only for one of the reasons in sections 27 to 29 and the individual is entitled to know:

- the reason for refusal (ie. exactly which reason is being relied on);
- the supporting grounds; and
- that they have a right to make a complaint to the Privacy Commissioner and to seek an investigation and review of the refusal (section 44).

There are a number of legitimate reasons for refusal. Most are unlikely to be relevant to many requests for health information made to health agencies and are not mentioned here. Comment is provided for several reasons, which arise more frequently. Staff responsible for reviewing access requests should, of course, familiarise themselves with all relevant provisions, not merely those noted here.

27(1)(c) – disclosure would be likely to prejudice the maintenance of the law, including prevention, investigation and detection of offences, and the right to a fair trial

Maintenance of the law is not limited to criminal proceedings and may apply where, say, an entitlement to a benefit under statute is administered by a statutory body or where criminal activity is suspected.

A decision to withhold information under section 27(1)(c) may be affected by the timing of the request. For instance, information might be withheld because its release would be likely to prejudice an ongoing fraud investigation by ACC, but the same could not be said once the investigation is complete and a decision made about what actions should be taken.

27(1)(d) – disclosure would be likely to endanger the safety of any individual

"Would be likely" to endanger safety means there need be no more than a distinct or significant possibility of the harm occurring. The safety risk might relate to the individual concerned, staff members, families or other people, and the risk must be a risk of physical harm (rather than, say, emotional or cultural harm).

29(1)(a) – disclosure would involve the unwarranted disclosure of the affairs of another individual

The rule 6 right of access is limited to information about the requester. However, sometimes that information is inextricably linked with information about another person.

For instance, 'mixed information' – that is, information about two or more people – may be created through the use of joint counselling sessions or because one person has referred to another in the course of treatment. If the information cannot be separated out by the deletion of identifying details, agencies need to decide whether releasing the mixed information to the requester would involve an unwarranted disclosure of the affairs of the other person. Essentially, section 29(1)(a) requires agencies to strike a balance between the privacy interests of the requester and the other person.

2: Health information privacy rules

Some issues that might need to be considered in striking this balance are:

- the nature and sensitivity of the information;
- whether one or both of the parties was promised confidentiality;
- the nature of the relationship between the requester and the other person;
- the likely reaction of the other person to the disclosure;
- the other person's views about giving access (if known, or able to be ascertained); and
- whether there are competing public interests warranting disclosure.

29(1)(b) – disclosure of evaluative material (or of the identity of the person who supplied it) would breach a promise of confidentiality to the person supplying the information

The disclosure of the information or of information identifying the person who supplied it, being **evaluative material**, would breach an express or implied promise:

(i) which was made to the person who supplied the information; and

(ii) which was to the effect that the information or the identify of the person who supplied it or both would be held in confidence.

"Evaluative material" is very narrowly defined in section 29(3) of the Privacy Act (see appendix). Note also that the material must be compiled *solely* for the limited purposes set out in section 29(3). For instance, information obtained to determine whether to insure an individual *is* evaluative material, while information obtained to determine whether to pay out on a particular insurance claim is *not* (section 29(3)(c)).

29(1)(c) – disclosure would be likely to prejudice the physical or mental health of that individual

Agencies seeking to rely on this exception must consult with the individual's medical practitioner where practicable. Where it is not practicable to do so, it may still be possible to conclude that the disclosure would be likely to prejudice the individual's physical or mental health. In any case, the information must relate to the individual's physical or mental health.

Sometimes more than one medical practitioner may be involved in a person's care and the question will arise as to who should be consulted. Each may have sufficient expert knowledge of the requester's medical condition to assist the agency in making its decision. However, the provision anticipates consulting the *individual's* medical practitioner, someone whose primary ethical duty is to the individual (rather than, say, a person engaged to examine the requester by an insurance company, the Police or a court). This is most likely to be the person's general practitioner or a specialist with whom the individual has more than a passing doctor/patient relationship.

29(1)(d) – disclosure would be contrary to the individual's interests (where the individual is under 16)

Individuals, whatever their ages, are entitled to access their personal health information. If releasing information to an individual under 16 would be contrary to that person's interests, consider whether all of the information must be withheld, or whether part of it could be released without prejudicing their interests. It may be possible to release part of the information, or to summarise or rephrase it so that its release would not be as potentially harmful.

29(2) – the information is not readily retrievable; does not exist or cannot be found; is not held and is not believed to be held by another agency etc

A proper search for the information must have been made before the request may be refused on the basis that the information is not readily retrievable, does not exist or cannot be found. Agencies should consider:

- what steps have been taken to locate the information;
- whether the file has been traced;
- whether checks have been made with all people who had or are likely to have had the file;
- whether the information is likely to have been destroyed; and
- whether the requester can further particularise his or her request and whether the information that is able to be located (if any) is of any assistance.

If it appears that the information has been lost because of inadequate security safeguards the requester could make a complaint that the agency has not taken reasonable steps to protect the information against loss (rule 5).

Before declining a request on the basis that the agency does not hold the information and does not believe either that it is held by any other agency or that it is more closely connected with another agency's functions, the agency could check with other potentially relevant agencies to see if they hold the type of information being sought.

FORM OF ACCESS (SECTION 42)

The information requested may be made available in any number of ways:

- by inspecting a document;
- as a printed or electronic copy of a document;
- by viewing an x-ray, CAT, PET or MRI scan;
- by watching videotape, hearing audio tape etc;
- on a transcript;
- as an excerpt or written summary; or
- orally.

2: Health information privacy rules

Sometimes a record of information could be safely loaned to an individual for a period. However, the right is one of access, not ownership. Individuals cannot insist that the original documents be given to them, although they can ask to inspect originals.

The health agency should try to make the health information available to the individual in the form requested (section 42(2)). However, access may be made available in a different form if providing it in the form requested would:

- impair efficient administration;
- be contrary to any legal duty of the agency in respect of the document; or
- prejudice the interests protected by sections 27, 28 or 29 of the Privacy Act.

In determining whether providing information in a particular way would impair efficient administration, issues such as the following need to be considered:

- if the requester wants a copy, how much information is to be copied, how long is that likely to take and is a person available to do it? and
- if the requester wants to see the original file, is that likely to require a person to sit with the requester and is that person going to be available for the required time?

It may be possible to satisfy a requester by providing an inexpensive digital copy of his or her medical records. However, this will also depend on whether the requester has the technical skills and equipment to make use of information provided in this way. Given the section 38 obligation to provide assistance to requesters, it is advisable to explore with the requester what method of access they will find most useful. Requesters are entitled to get their information in the manner that best suits them, subject to the limitations above.

Where information is not provided in the form requested by the individual, the health agency must give the individual the reason for not providing the information in that form, and, if requested, the grounds in support of that reason, provided that giving the grounds does not prejudice the interests protected by sections 27, 28 or 29.

Where an individual has sought access to medical records, it may sometimes be appropriate for a suitable person to be available to assist in interpreting the information and to answer any questions from the individual.

DELETION OF INFORMATION FROM DOCUMENTS RELEASED (SECTION 43)

If there is a good reason for withholding some of the information in a document, a copy of the full document may be made available with any necessary deletions or alterations (eg. if part of the document relates to someone else). Where this happens, the agency must give the individual the reason for withholding the information and, if requested, the grounds for doing so. The agency should also advise the individual of any internal complaints procedures and of the right to complain to the Privacy Commissioner.

2:

Health information privacy rules

ACCESS TO RESEARCH TRIALS

Participants in medical research are generally given the results at the conclusion of the study. Occasionally a participant may seek access to personal information while the research is still continuing. If there is readily retrievable personal information, such requests must be dealt with in accordance with the Privacy Act. However, where access to the personal information would prejudice the validity of the research design, the research participants should be told this at the time their consent is sought to participate in the study. If a participant insists on access to the information, this could be treated as a withdrawal from the research, and access provided in accordance with rule 6.

See clause 6 (charges) and Privacy Act, Part 4 (sections 27 to 32), Part 5 (sections 33 to 45) and Health Act, section 22F. Opinions reached in personal access cases by the Privacy Commissioner and, prior to 1993, the Ombudsmen can be found in the Privacy Commissioner's case notes and the case notes of the Ombudsmen. Privacy officers and legal advisers may wish to refer to the detailed legal guidance in *Privacy Law and Practice.*

2:
Health information privacy rules

Rule 7: CORRECTION OF HEALTH INFORMATION

(1) Where a health agency holds health information, the individual concerned is entitled:

(a) to request correction of the information; and

(b) to request that there be attached to the information a statement of the correction sought but not made.

(2) A health agency that holds health information must, if so requested or on its own initiative, take such steps (if any) to correct the information as are, in the circumstances, reasonable to ensure that, having regard to the purposes for which the information may lawfully be used, it is accurate, up to date, complete, and not misleading.

(3) Where an agency that holds health information is not willing to correct the information in accordance with such a request, the agency must, if so requested, take such steps (if any) as are reasonable to attach to the information, in such a manner that it will always be read with the information, any statement provided by the individual of the correction sought.

(4) Where the agency has taken steps under subrule (2) or (3), the agency must, if reasonably practicable, inform each person or body or agency to whom the health information has been disclosed of those steps.

(5) Where an agency receives a request made under subrule (1), the agency must inform the individual concerned of the action taken as a result of the request.

(6) The application of this rule is subject to the provisions of Part 5 of the Act (which sets out procedural provisions relating to correction of information).

(7) This rule applies to health information obtained before or after the commencement of this code.

Note: *An action is not a breach of this rule if it is authorised or required by or under law: Privacy Act 1993, section 7(4).*

COMMENTARY

Individuals have a right to request correction of their health information or that a statement of a correction sought but not made be attached to their file. Correction is an important right as it can reduce the possibility of receiving treatment on the basis of inaccurate information. Correction may involve altering personal information by way of amending or correcting, deleting or adding information.

Agencies also have an obligation under rule 8 to take reasonable steps to ensure that information they propose to use is accurate, regardless of whether a correction request has been made.

PROCEDURAL PROVISIONS RELATING TO CORRECTION OF PERSONAL INFORMATION

Procedural provisions relating to the correction of information are covered by Part 5 of the Privacy Act. A detailed understanding of these requirements can be obtained only by referring directly to the Privacy Act. See also the commentary to rule 6 in respect of:

- identity of person requesting correction (section 45);
- urgent requests (section 37);
- assistance to be given (section 38);
- transfer of requests (section 39);
- decisions on requests (section 40); and
- extension of time limits (section 41).

Agencies that receive a correction request must consider the request and respond by either:

- agreeing to it;
- refusing it and advising the individual of the right to complain to the Privacy Commissioner; or
- suggesting an alternative solution such as attaching a statement of the correction sought by the individual.

The right to seek correction is *not* dependent on an individual having been granted access.

Individuals do not have the right to make changes themselves on documents containing health information. While those records remain with the agency, it is the agency that considers any request and, if any change is needed, it is the agency that will make the change. Where a change is made there should, as a matter of good practice, be an administrative record of who authorised the change and when. Consider developing a standard paper or electronic form to record such information as:

- why the change or addition is sought;
- who should be notified of the change or addition; and
- whether the individual wishes to have a copy of the amended or added record.

2: Health information privacy rules

REASONS FOR REFUSAL

Where a request for correction is refused the individual must be informed of the:

- reasons for refusal;
- supporting grounds for refusal;
- right to request the attachment to the information of a statement provided by the individual of the correction sought; and
- right to complain to the Privacy Commissioner and to seek an investigation and review of the decision.

Reasons for refusing a request for correction might include that:

- the health agency is satisfied the information is correct;
- the information is clearly identified as opinion material and correctly represents the opinion held at the time (eg. an assessment of an individual's risk of suicide or a diagnosis) – removing or changing the earlier information would leave a course of action unexplained; and
- the information was believed to be correct at the time it was made, circumstances have changed, and there is no means of now verifying its accuracy.

NOTICE OF CORRECTION SOUGHT TO BE ATTACHED

Where a health agency is not willing to correct information when requested, it must take reasonable steps to attach to the information a statement (normally provided by the individual) of any correction sought and not made. The agency might helpfully offer to prepare for the individual's approval a suitable draft statement based on what the individual has alleged is the case. This obligation to attach a notice of correction to, potentially, any part of a file should be taken into account when designing and implementing new computer and file handling systems.

REQUIREMENT TO INFORM OTHERS OF CORRECTION

As far as is reasonably practicable, the health agency must take steps to inform other people and agencies to whom the information has been disclosed of any correction made. Sometimes an individual's help may be sought to do this. The agency is also, of course, required to tell the requester of its decision on the request for correction (see section 40).

See rule 8 and Privacy Act, Part 5 (sections 33 to 45). See also clause 6 (charges). Discussion of cases concerning the right of correction under the Privacy Act, and earlier cases under the Official Information Act, can be found in the Privacy Commissioner's case notes and the Ombudsmen's case notes.

Rule 8: ACCURACY ETC OF HEALTH INFORMATION TO BE CHECKED BEFORE USE

(1) A health agency that holds health information must not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date, complete, relevant, and not misleading.

(2) This rule applies to health information obtained before or after the commencement of this code.

Note: *An action is not in breach of this rule if it is authorised or required by or under law: Privacy Act 1993, section 7(4).*

COMMENTARY

Rule 8 aims to protect individuals by requiring agencies that hold health information to check its accuracy before using it. What is required in terms of checking will vary depending on matters like:

- the proposed use;
- the age of the information and the reliability of its source;
- the practicalities of verifying accuracy or currency; and
- the probability, severity and extent of potential harm for the individual should the information be inaccurate.

PURPOSE FOR WHICH INFORMATION TO BE USED

The steps that it is reasonable to take to check information will vary depending upon the proposed use. If the information is to be aggregated for statistical purposes, few or no checks might be needed, particularly if the checking process would unnecessarily intrude on the individual's privacy. By contrast, rigorous checks will be appropriate if decisions on health care entitlements or treatment alternatives are to be based on that information.

ACCURACY AND COMPLETENESS

The accuracy of health information is important for all purposes for which health information is used – care and treatment, administration, monitoring quality of care, training and education. Reasonable steps for ensuring accuracy might include:

2: Health information privacy rules

- having individuals check the accuracy of the health information they supply at the time it is collected;
- informing individuals of their own responsibility to keep their name and address information up to date;
- where information is computerised, adopting a data outlier program to identify when data falls outside expected ranges and values; and
- training staff appropriately.

ACCURACY AND COMPLETENESS WHERE INFORMATION NOT COLLECTED FROM INDIVIDUAL

Health agencies may have greater problems taking steps to ensure accuracy and completeness where information is not collected directly from an individual but is provided by another health agency. If the information is going to be used, agencies dealing directly with the individual concerned should check the accuracy of the information with the individual at an early opportunity, if practicable. Consideration should be given to recording the source of the information on the file.

UP TO DATE

In developing procedures to update health information, health agencies need to consider whether:

- the individual might be harmed by the information being out of date;
- treatment might be affected by the information being out of date; and
- a health agency to which the information might be disclosed might treat the individual differently if the information was updated.

Information that is likely to change, such as an address, should be checked – perhaps at each encounter with the individual.

See rules 3 and 7.

Rule 9: RETENTION OF HEALTH INFORMATION

(1) A health agency that holds health information must not keep that information for longer than is required for the purposes for which the information may lawfully be used.

(2) Subrule (1) does not prohibit any agency from keeping any document that contains health information the retention of which is necessary or desirable for the purposes of providing health services or disability services to the individual concerned.

(3) This rule applies to health information obtained before or after the commencement of this code.

Note: *An action is not a breach of this rule if it is authorised or required by or under law: Privacy Act 1993, section 7(4).*

COMMENTARY

Normally health records are created for the care and treatment of an individual. However, as discussed in the commentary to rule 1, such records are often also required for the lawful purposes of administration, monitoring, training and education. There may be a good reason for retaining records well after they have ceased to be relevant for the primary purpose of care and treatment. Archived and stored information should be regularly assessed to see if it is still required.

Rule 9 does not require that agencies only keep health information for as long as required for the *original* purpose for which it was collected or obtained. Information may be kept as long as there remains *some* lawful purpose. However, information kept beyond the expiry of its original purpose risks 'function creep'. See the commentary to rule 1 for more discussion of the meaning of "lawful" in the context of the code.

Many people are equally concerned that their health information may be disposed of too soon as retained for too long a period. Health information must be retained under the express requirements of certain enactments, such as:

- the Health (Retention of Health Information) Regulations 1996;
- clause 58 of the Medicines Regulations 1984; and
- the Public Records Act 2005.

2: Health information privacy rules

District Health Boards are subject to the General Disposal Authority for District Health Boards DA262. The Disposal Authority sets out specific retention times for each category of health record and is available on the Archives New Zealand website www.archives.govt.nz.

The Health (Retention of Health Information) Regulations require health records to be retained by all health agencies for a minimum of 10 years. Extracts from these regulations are set out in the appendix.

The individual concerned may also expressly request the retention of health records or may ask to have the records after they are no longer needed by the health agency.

Where health information is stored for long periods (eg. for research or legal purposes, rather than for day-to-day care and treatment and administration) it should be held in secure storage (eg. in a secure and locked filing cabinet, a warehouse or off-line).

When disposing of information, carefully consider rule 5, especially rule 5(1)(c), which requires information to be disposed of in a manner that preserves the privacy of the individual.

HEALTH RESEARCH

Researchers wishing to keep identifying information or identified specimens longer than required for the original research project would be expected to obtain the agreement of an ethics committee.

Where the principal researcher in a project changes responsibilities or moves, responsibility for the security or disposal of the information needs to be assigned to that person's successor, or to the head of the department or institution. For the disposal of records involving Māori information, where a kaitiaki group has been established to act as guardian of Māori information in the area of research, the kaitiaki group should be consulted.

See rules 1, 5 and 10. See also the Health (Retention of Health Information) Regulations 1996 and the Public Records Act 2005.

Rule 10: LIMITS ON USE OF HEALTH INFORMATION

(1) A health agency that holds health information obtained in connection with one purpose must not use the information for any other purpose unless the health agency believes, on reasonable grounds,—

(a) that the use of the information for that other purpose is authorised by—

(i) the individual concerned; or

(ii) the individual's representative where the individual is unable to give his or her authority under this rule; or

(b) that the purpose for which the information is used is directly related to the purpose in connection with which the information was obtained; or

(c) that the source of the information is a publicly available publication; or

(d) that the use of the information for that other purpose is necessary to prevent or lessen a serious threat to—

(i) public health or public safety; or

(ii) the life or health of the individual concerned or another individual; or

(e) that the information—

(i) is used in a form in which the individual concerned is not identified; or

(ii) is used for statistical purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(iii) is used for research purposes (for which approval by an ethics committee, if required, has been given) and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(f) that non-compliance is necessary—

(i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(g) that the use of the information is in accordance with an authority granted under section 54 of the Act.

(2) This rule does not apply to health information obtained before 1 July 1993.

Note: *An action is not a breach of this rule if it is authorised or required by or under law: Privacy Act 1993, section 7(4). Rule 10(2) was amended by Amendment No 1.*

2: Health information privacy rules

COMMENTARY

Rule 10 limits the uses to which health information can be put. Its focus is on purpose: the basic rule is that information obtained for one purpose cannot be used for any other purpose unless an exception applies.

Agencies that have complied with rule 1 will have clear purposes for having information. Rule 10 allows them to use the information for those purposes. Agencies that have collected the information directly from the individual concerned should have made the individual aware of those purposes amongst the other matters required by rule 3.

EXCEPTIONS TO RULE 10

There are a number of exceptions to the general rule contained in rule 10. Some of the exceptions mirror the exceptions to other rules.

Information may be used for other purposes where:

(a) An individual authorises use for other purposes

For example, where health information has been obtained for care and treatment purposes, the agency might ask the individual to authorise use for other purposes such as research. Individuals are free to refuse to authorise use for a new purpose. Individual authorisation is usually preferable to relying on some other exception to rule 10. Authorisation means an active agreement to a use rather than a passive acquiescence. In order to actively authorise something, the individual needs to have a general understanding of what he or she is agreeing to.

(b) Directly related purpose

This may include, for example, certain administrative uses.

(c) Information sourced from a publicly available publication

Information which has been obtained from a publicly available publication such as a telephone directory, published report or public register (eg. register of births, deaths and marriages) can be used for a new purpose, as can information obtained from a publicly available website or other internet resource. This exception applies only if the agency has actually obtained the information *from* the publicly available publication. It is not sufficient that information held by the agency *could* alternatively have been obtained from a publicly available source.

(e)(i) The information will not identify the individual

This exception allows, for example, the use of health records for another purpose within the agency provided the personally identifiable information has been removed. The rule also permits use for statistical or approved research purposes provided information is not published in a form that could reasonably be expected to identify the individual. Seeking ethics committee approval will help ensure that privacy and other concerns are suitably addressed in particular research projects.

Another example of legitimate use of information where the individual is not identified might be where a student sees a patient (with consent) and later writes up the notes as a case history without identifying the patient.

(e)(iii) The information is sought for research purposes

This exception permits health information obtained for one purpose to be used for health research (approved by an ethics committee, if required).

Information obtained in connection with one research purpose may be used for another research project only if one of the exceptions to rule 10 applies, for example:

- if the individual concerned agrees – rule 10(1)(a);
- if the approval of an ethics committee is obtained for the new research proposal – rule 10(1)(e).

The requirements of an ethics committee may be more stringent than the legal requirements of this code.

(f)(ii) The information is required for court proceedings

This exception is limited by provisions of the Evidence Act, which prohibit disclosure in court of certain protected communications except with the consent of the patient (refer to section 59 of the Evidence Act 2006 – set out in the appendix).

(g) Authority under section 54

In certain circumstances the Privacy Commissioner may authorise an agency to use information in a way that would otherwise breach rule 10. The power is reserved for cases where an exemption will substantially benefit the public interest or involve a clear benefit to the individual concerned. However, the Commissioner cannot grant an authority if the individual concerned has specifically refused to authorise the use. Section 54 is designed for exceptional cases, rather than for ongoing situations. Agencies that believe a particular use is likely to breach rule 10 and that it is likely to be an ongoing use need to consider altering their procedures to bring the activity in line with rule 10.

See the Office of the Privacy Commissioner's "Guidance Note to Applicants seeking Exemption under Section 54 of the Privacy Act 1993", www.privacy.org.nz.

See rules 1 and 3.

2:

Health information privacy rules

Rule 11: LIMITS ON DISCLOSURE OF HEALTH INFORMATION

(1) A health agency that holds health information must not disclose the information unless the agency believes, on reasonable grounds, that—

(a) the disclosure is to—

(i) the individual concerned; or

(ii) the individual's representative where the individual is dead or is unable to exercise his or her rights under these rules; or

(b) the disclosure is authorised by—

(i) the individual concerned; or

(ii) the individual's representative where the individual is dead or is unable to give his or her authority under this rule; or

(c) the disclosure of the information is one of the purposes in connection with which the information was obtained; or

(d) the source of the information is a publicly available publication; or

(e) the information is information in general terms concerning the presence, location, and condition and progress of the patient in a hospital, on the day on which the information is disclosed, and the disclosure is not contrary to the express request of the individual or his or her representative; or

(f) the information to be disclosed concerns only the fact of death and the disclosure is by a health practitioner or by a person authorised by a health agency, to a person nominated by the individual concerned, or the individual's representative, partner, spouse, principal caregiver, next of kin, whānau, close relative, or other person whom it is reasonable in the circumstances to inform; or

(g) the information to be disclosed concerns only the fact that an individual is to be, or has been, released from compulsory status under the Mental Health (Compulsory Assessment and Treatment) Act 1992 and the disclosure is to the individual's principal caregiver.

(2) Compliance with subrule (1)(b) is not necessary if the health agency believes on reasonable grounds that it is either not desirable or not practicable to obtain authorisation from the individual concerned and that—

(a) the disclosure of the information is directly related to one of the purposes in connection with which the information was obtained; or

(b) the information is disclosed by a health practitioner to a person nominated by the individual concerned or to the principal caregiver or a near relative of the individual concerned in accordance with recognised professional practice and

the disclosure is not contrary to the express request of the individual or his or her representative; or

(c) the information—

(i) is to be used in a form in which the individual concerned is not identified; or

(ii) is to be used for statistical purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(iii) is to be used for research purposes (for which approval by an ethics committee, if required, has been given) and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(d) the disclosure of the information is necessary to prevent or lessen a serious threat to—

(i) public health or public safety; or

(ii) the life or health of the individual concerned or another individual; or

(e) the disclosure of the information is essential to facilitate the sale or other disposition of a business as a going concern; or

(f) the information to be disclosed briefly describes only the nature of injuries of an individual sustained in an accident and that individual's identity and the disclosure is—

(i) by a person authorised by the person in charge of a hospital; or

(ii) to a person authorised by the person in charge of a news medium—

for the purpose of publication or broadcast in connection with the news activities of that news medium and the disclosure is not contrary to the express request of the individual concerned or his or her representative; or

(g) the disclosure of the information—

(i) is required for the purposes of identifying whether an individual is suitable to be involved in health education and so that individuals so identified may be able to be contacted to seek their authority in accordance with subrule (1)(b); and

(ii) is by a person authorised by the health agency to a person authorised by a health training institution; or

(h) the disclosure of the information is required—

(i) for the purpose of a professionally recognised accreditation of a health or disability service; or

(ii) for a professionally recognised external quality assurance programme; or

(iii) for risk management assessment and the disclosure is solely to a person engaged by the agency for the purpose of assessing the agency's risk—

and the information will not be published in a form which could reasonably be expected to identify any individual nor disclosed by the accreditation, quality assurance, or risk management organisation to third parties except as required by law; or

(i) non-compliance is necessary—

(i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(j) the individual concerned is or is likely to become dependent upon a controlled drug, prescription medicine, or restricted medicine and the disclosure is by a health practitioner to a Medical Officer of Health for the purposes of section 20 of the Misuse of Drugs Act 1975 or section 49A of the Medicines Act 1981; or

(k) the disclosure of the information is in accordance with an authority granted under section 54 of the Act.

(3) Disclosure under subrule (2) is permitted only to the extent necessary for the particular purpose.

(4) Where, under section 22F(1) of the Health Act 1956, the individual concerned or a representative of that individual requests the disclosure of health information to that individual or representative, a health agency—

(a) must treat any request by that individual as if it were a health information privacy request made under rule 6; and

(b) may refuse to disclose information to the representative if—

(i) the disclosure of the information would be contrary to the individual's interests; or

(ii) the agency has reasonable grounds for believing that the individual does not or would not wish the information to be disclosed; or

(iii) there would be good grounds for withholding the information under Part 4 of the Act if the request had been made by the individual concerned.

(5) This rule applies to health information about living or deceased persons obtained before or after the commencement of this code.

(6) Despite subrule (5), a health agency is exempted from compliance with this rule in respect of health information about an identifiable deceased person who has been dead for not less than 20 years.

Note: *Except as provided in rule 11(4), nothing in this rule derogates from any provision in an enactment which authorises or requires information to be made available, prohibits or restricts the availability of health information, or regulates the manner in which health information may be obtained or made available: Privacy Act 1993, section 7. Note also that rule 11, unlike the other rules, applies not only to information about living individuals, but also about deceased persons: Privacy Act 1993, section 46(6).*

Note: *Rule 11(1)(f) was amended by Amendment No 4. Rule 11(1)(g) was inserted by Amendment No 3, which also amended rule 11(6). The terms "health professional" and "registered health professional" were changed to "health practitioner" by Amendment No 6.*

COMMENTARY

Rule 11 places limits on the disclosure of information. Unlike rule 6, it does not *oblige* an agency to disclose information. Instead it *allows* disclosure if an exception to the rule applies. However, an agency may decide not to disclose even though an exception to the rule applies. The decision to disclose, when permitted by the rule, remains within the agency's discretion.

A number of factors may bear upon that decision, such as the ethical code of the particular health professional or duties of confidentiality. Ethical and professional obligations might impose stricter limits on disclosure than those of rule 11.

Under the code, individuals do not have a general right of veto over the disclosure of their health information. However, a number of exceptions within rule 11 allow certain disclosures, *except* where the individual has vetoed that disclosure. That veto only affects the use of that particular exception and does not prevent disclosure where another exception applies.

Health agencies should take steps to ensure that all staff (including volunteers) are familiar with the grounds for disclosure of health information, their own responsibilities and the agency's procedures and safeguards.

RULE 11 PERMITTED DISCLOSURE

A health agency may disclose health information where it believes on reasonable grounds that one of the exceptions set out in rule 11(1) apply:

(1)(a) & (b) Disclosure is to, or authorised by, the individual concerned

If disclosure is to the individual concerned privacy issues are unlikely to arise. However, care must be taken in disclosing information to ensure that information about other individuals is not disclosed in breach of rule 11.

Authorisation need not be in writing, but the agency disclosing the information must believe on reasonable grounds that disclosure has been authorised. Note that

2:

Health information privacy rules

authorisation means more than just consent; it implies a general understanding of what is being agreed to by the individual concerned.

Information may be disclosed to a representative, or disclosure authorised by a representative, where the individual cannot exercise his or her rights under the code. "Representative" is defined in clause 3. Under section 22F of the Health Act 1956, a representative also has the ability to directly request access to information about an individual. See 'Requests under section 22F of the Health Act' page 67.

Hospitals might seek an individual's authorisation to certain disclosures by involving the individual in the preparation of a discharge plan.

Disclosure authorised by the individual, or by his or her representative, is almost always preferable to relying on some other ground for disclosure in rule 11.

(c) Disclosure is a purpose for which the information was obtained

This exception includes instances where information is required for further treatment of the individual or where the information is required for administrative aspects of care and treatment, or for monitoring that care and treatment. If information was obtained for an anticipated purpose, under rule 3 the individual should already have been notified of that purpose.

(d) Information sourced from a publicly available publication

Information that has been obtained from a publicly available publication such as a website, telephone directory, published report or public register (eg. register of births, deaths and marriages) can be disclosed. This exception applies only if the agency has actually sourced the information from the publicly available publication. It is not sufficient that information held by the agency might alternatively have been obtained from a publicly available publication.

(e) Disclosure of general information about a hospital patient on a particular day

Many hospitals have operational procedures (such as a patient enquiries line) for the disclosure of general information about an individual's presence and location in hospital and condition. General information may be conveyed, such as confirmation that a named patient has been admitted and that he or she is comfortable, stable, etc. Location information may also be provided to assist visitors. This exception does not permit the disclosure of detailed particulars of the patient's treatment or prognosis.

The individual may veto the disclosure of such information. For most non-urgent admissions hospitals should make their policy known in advance – perhaps through their admission forms – so that patients can choose to veto or "opt-out" of this potential disclosure of their information.

(g) Release from compulsory status

Health agencies may inform an individual's principal caregiver of the individual's release, or imminent release, from compulsory status under the Mental Health (Compulsory Assessment and Treatment) Act 1992.

"Principal caregiver" is defined in clause 3 as the friend of the individual or the member of the individual's family group or whānau who is most evidently and directly concerned with the oversight of the individual's care and welfare.

Information about release from compulsory status can be disclosed under this exception, However, principal caregivers and other family members may well want to know more than the bare fact of release, and this extra disclosure would not be permitted by rule 11(1)(g). Therefore, additional disclosures should be addressed by the preparation of a discharge plan with the individual's involvement.

RULE 11(2) FURTHER PERMITTED DISCLOSURES

Disclosure is also allowed under subrule (2) in a number of circumstances where it is not desirable or practicable to obtain individual authorisation. This covers circumstances where the individual may not be competent to provide their consent, cannot be found, or has explicitly refused to provide consent.

The requirement to, where possible, obtain authorisation before disclosure is more stringent than the equivalent provision in the Privacy Act. This is because of the perceived sensitivity of health information and the importance of maintaining individual autonomy in respect of it.

(2)(a) Disclosure for directly related purpose

Directly related purposes are purposes closely connected with the purpose for which the information was collected. They are purposes that could reasonably be assumed to be within the expectations of the person from whom the information was collected. This may include, for example, disclosure of information for peer review and quality audit.

Disclosure for debt collection (or limited disclosure essential for reimbursement by a funder) would normally be a purpose directly related to billing purposes (which might involve disclosure of name, address and other limited details).

(b) Disclosure of information to nominated person, principal caregiver or near relative

Health agencies will need to have clear operational procedures in place to establish the identity of the person to whom the information is being disclosed. While individuals do not generally have a legal right of veto over the disclosure of their health information, when disclosing information under this provision regard should be had to any express wishes of the individual concerned.

Difficulties may arise with patients who move in and out of psychiatric institutions and the care of a family member or caregiver. Often at the time of re-admission such patients may be hostile to their caregivers and veto the giving of any information to them. There is no easy solution to this issue but the rule does require respect for clear instructions by the patient.

2: Health information privacy rules

Discretion and skill should be exercised by agencies when broaching the subject (eg. obtaining "standing" instructions during a calm lucid period rather than in the heat of an angry re-admission) and in discussing the limits of any refusal to authorise disclosure (eg. acknowledging the patient's right to keep details of treatment private while negotiating to seek permission to tell a family member at least that the patient is okay). Even where the patient does refuse authorisation to disclose, the matter should be raised again later and not left in an unsatisfactory state.

Where a clinician considers a psychiatric patient does not currently have the mental capacity to give or withhold consent, disclosure may be made to, or with the authority of, a representative (see rule 11(1)).

(c)(i), (ii) Individual not identified

Health practitioners sometimes use actual case studies in peer group discussions (only with other practitioners) to improve competence generally. Sometimes patient authorisation is obtained. Exception (c)(i) can be relied on when it is not practicable to obtain authorisation and when the individual concerned is not identified (eg. by reading extracts from the notes or circulating copies with identifying details masked).

The statistical purposes exception in (c)(ii) also prohibits any publication in a form that could reasonably be expected to identify any individual.

Additional to this provision, section 22H of the Health Act permits the disclosure of "anonymised" health information that does not permit the identification of the person to whom it relates.

(c)(iii) Disclosure for research purposes

When an agency is approached by a researcher seeking the disclosure of health information, it first needs to satisfy itself that ethical approval has been obtained (if required) and that the information will not be published in a form that could identify any individual. The agency being asked to disclose information will probably also want to be satisfied as to security safeguards and the manner of approach to the individual (if any). These issues should be anticipated by the researcher and addressed expressly within the protocol, with the ethics committee and in the approach to the agency.

A researcher should also anticipate any disclosures inherent in a research proposal and address those in the protocol for the ethics committee's consideration. The committee may wish to place conditions on the use or disclosure of the information.

See also Health Research Council, *Guidelines on Ethics in Health Research* (2005), Part 6, "Health Research and Privacy: Guidance Notes for Health Researchers and Ethics Committees" (printed in 1/4 *Human Rights Law and Practice*, March 1996, 196-210), and the currently applicable Ministry of Health operational guidelines for ethics committees.

(d) Disclosure necessary to prevent or lessen a serious threat to public health or public safety or the life or health of an individual

This exception sets a high bar for disclosure, and should not be used lightly. In order to disclose under this exception, an agency needs to believe on reasonable grounds that it is not practicable or desirable to obtain individual authorisation and that:

- there is a serious threat to public health, public safety or the life or health of an individual;
- the disclosure of the information would prevent or lessen that threat; and
- the disclosure of the information is necessary to prevent or lessen the threat.

When considering whether the disclosure is "necessary", agencies should consider whether the threat could be prevented or minimised in some way that does not involve the release of sensitive or confidential information.

The disclosure must be made to a person who can do something to prevent or lessen the threat. Disclosure to someone who does not have such power may merely be an inroad into medical confidence and privacy that does not carry with it any corresponding assurance of benefit to the public interest.

Even if disclosure is warranted, it should only be to the extent necessary to prevent or lessen the threat – rule 11(3). A decision to disclose will only justify the disclosure of information that is necessary to prevent or lessen the threat. Agencies need to decide how much information needs to be disclosed. It may not be necessary for the whole file to be disclosed.

Generally, if there is an official with powers to deal with such a threat, such as a police officer, then disclosure to that responsible authority will be an appropriate response. As a matter of good practice, the purpose of the disclosure should be made clear so that the person receiving the information knows the limited purpose to which it can be put.

(e) Disclosure essential to facilitate sale of business

It is unlikely that disclosure of personally identifiable health information would be essential to facilitate the sale of a business. In most cases, non-identifiable information should satisfy all reasonable requirements. Any information obtained must not be used for any purpose other than to facilitate the sale.

(f) Disclosure by hospital to news media of accident victim injuries

Clear procedures are needed to establish the good faith of the person making a request and to give effect to a veto by the patient or representative. There is benefit in liaising with the local news media to ensure these procedures are known and workable. The exception allows only for the release of very basic details of injuries where it is

2:

Health information privacy rules

not practicable or desirable to seek authorisation. Where greater detail is proposed to be given to the media (ie. with authorisation of individual or representative, as may happen with public figures) suitable staff briefing and management involvement should help avoid difficulties with the media.

(g) Disclosure in relation to health education

Express authorisation will normally be required before involving patients in health education. However, sometimes it will be necessary for the educator to view the records of possible subjects to check whether they would be suitable. This exception will allow the chosen subjects to be approached to see if they are willing to participate.

(h) Accreditation, quality assurance or risk assessment programmes

To ensure higher standards in the health and disability sectors, there is growing use of formal accreditation and quality assurance programmes. To carry these out it is sometimes necessary to disclose identifiable patient information – often on a random basis. See Health Practitioners Competence Assurance Act 2003, Part 3, for provisions concerning Ministerial authorised quality assurance activities in relation to health services provided by health practitioners.

The investigation of specific complaints would not fall under any of these categories, nor would the exercise of statutory powers to investigate fraud or verify payment (eg. section 22G Health Act, which is set out in the appendix).

(i) Non-compliance necessary for maintenance of law, enforcement of law, protection of public revenue, or conduct of proceedings

Health information may be disclosed if it is necessary to avoid prejudice to the maintenance of the law by a public sector agency such as the Police or agencies with laws to administer, such as ACC.

The Evidence Act 2006 prohibits the disclosure by medical practitioners or clinical psychologists of some information in civil and criminal proceedings (section 59).

See also section 22C of the Health Act, set out in the appendix, which allows (but does not require) the disclosure of health information to certain statutory officials, on request.

(j) Drug seekers

Section 20 of the Misuse of Drugs Act 1975 and section 49A of the Medicines Act 1981 are set out in the appendix. Consideration should also be given to the rule 3 obligations, if applicable, at time of information collection. It is suggested that a warning notice be displayed in the reception or waiting room explaining that information about suspected drug seekers may be disclosed, where appropriate.

(k) Authority under section 54

In rare circumstances, the Privacy Commissioner may authorise an agency to disclose information in a way that would otherwise breach rule 11. This power is reserved for

cases where an exemption from the rule will substantially benefit the public interest or involve a clear benefit to the individual concerned. The Commissioner *cannot* grant an authority if the individual has specifically refused to authorise the disclosure.

Section 54 is designed for exceptional cases, rather than for ongoing situations. Agencies that believe a particular type of disclosure is likely to breach rule 11 and that the same matter is likely to recur need to consider altering their procedures to bring the activity in line with rule 11 (for example, by obtaining individual authorisation in advance) or advising individuals at the point of collection of the proposed disclosure (rule 3).

See the Office of the Privacy Commissioner's "Guidance Note to Applicants seeking Exemption under Section 54 of the Privacy Act 1993", www.privacy.org.nz.

SUBRULE (3): DISCLOSURE ONLY TO EXTENT NECESSARY

When disclosures are made without the authorisation of the individual concerned, the disclosure should be made only to the extent necessary to meet the particular purpose or permitted request. Ideally, requests for unauthorised disclosure should be satisfied without disclosing any personally identifying information at all, for instance by providing generic or anonymised information.

SUBRULE (4): REQUESTS UNDER SECTION 22F OF THE HEALTH ACT

Rule 11(4) modifies the effect of section 22F(1) of the Health Act 1956, which is set out in the appendix. Section 22F(1) requires any person holding health information to disclose that information in certain circumstances.

The people who may request a disclosure of information under section 22F are:

- the individual concerned;
- the individual's representative; and
- a person who is providing, or is going to provide, health or disability services to the individual.

Under section 22F, a valid request may only be refused where the holder of the information believes the individual does not want the information disclosed, where refusal is authorised by the Health Information Privacy Code, or where the person holding the information has a lawful excuse (such as a statutory obligation of confidentiality or one of the grounds in sections 27-29 of the Privacy Act) to refuse the request.

If the agency refuses the request a complaint may be lodged with the Privacy Commissioner under section 22F(4).

2: Health information privacy rules

Rule 11(4) requires section 22F requests from the individual concerned to be treated as if they were information privacy requests under rule 6. An agency *may* (but is not required to) refuse to disclose information to a representative if:

- the disclosures would be contrary to the individual's interests;
- the individual does not or would not want the information released; or
- there would be good grounds to refuse the individual concerned access under sections 27-29 of the Privacy Act.

Section 22F and its interactions with rule 11(4) are technically complex, but relatively straightforward in practice. For instance, the mother of an eight year old girl asks a GP to provide a copy of her daughter's test results. Because the child is under 16, the mother is considered to be her daughter's representative. Therefore, the GP must provide the information unless he or she believes that to do so would not be in the child's interest, or that the child would not wish the information to be disclosed.

If either of these is the case, the GP may refuse the mother's request. The GP may also refuse the request if one of the section 27-29 grounds for refusal applies (see commentary to rule 6, page 38). In any case, the GP would have to carefully consider his or her ethical obligation to the patient before acting contrary to the patient's expressed wishes.

Common sense and medical ethics suggest that consultation with the individual concerned, where practical, will be a vital step in resolving difficult section 22F dilemmas.

OTHER ENACTMENTS

A number of other enactments authorise or require personal information to be made available. Others prohibit or restrict disclosure of certain information. Some of these are set out in the appendix (eg. see sections 22C, 22D and 22F of the Health Act). It is possible here only to mention a few provisions. Agencies that are subject to these statutes should know of their existence.

Examples of enactments authorising or requiring disclosure

One example is section 11 of the Social Security Act 1964. Demands from the Ministry of Social Development under section 11 of the Social Security Act are constrained by the *Code of Conduct for Obtaining Information under Section 11 Social Security Act 1964.* For instance, the code does not permit the Ministry to seek, from a hospital or health professional, an opinion as to whether a beneficiary is married (or in a relationship in the nature of marriage). Nor is it entitled to seek information concerning any confidential communication to a health practitioner for the purpose of diagnosis or treatment. Copies of the code of conduct may be obtained from the Ministry of Social Development at www.msd.govt.nz. The Privacy Commissioner can investigate breaches of that code.

Sections 15 and 16 of the Children, Young Persons and Their Families Act 1989 authorise the reporting of suspected child abuse to a social worker or a member of the Police. These sections are reprinted in the appendix.

Section 18 of the Land Transport Act 1998 requires doctors and optometrists to notify the Director of Land Transport Safety if they know of someone who is likely to drive, but whose mental or physical condition is such that in the interests of public safety they should not be permitted to do so.

Section 19 of the Land Transport Act requires the person in charge of a hospital to notify the Director of Land Transport Safety if a person who holds a driver licence becomes subject to an in-patient compulsory treatment order under mental health legislation or becomes a special patient.

The Cancer Registry Act 1993 requires the person in charge of a laboratory to report positive cancer test results to the Director-General of Health.

Section 37 of the Victims Rights Act 2002 requires a victim of certain serious offences to be given notification of the escape or discharge of a person who has been compulsorily detained in a hospital because of the offence.

See the appendix for extracts from a number of statutes including, amongst others, the Privacy Act, Children, Young Persons and their Families Act, Evidence Act, Health Act, Medicines Act and Misuse of Drugs Act.

Official Information Act 1982

Public hospitals, the Ministry of Health and a number of other public bodies are subject to the Official Information Act 1982. Information held by such organisations can be requested under Part 2 of that Act and requests may be refused only for the reasons set out in it. However, requests made by individuals for information about themselves must be dealt with in accordance with the Privacy Act and this code.

When a request is made for official information (that is not about the requester), a public sector agency must consider the application under the Official Information Act. One of the purposes of the Official Information Act is to "protect official information to the extent consistent with the public interest and the preservation of personal privacy". Accordingly, one of the permitted reasons for withholding information is privacy. Section 9(2)(a) allows for information to be withheld if it is necessary to protect the privacy of a natural person, including a deceased natural person. If section 9(2)(a) applies, the agency must also consider whether in the particular circumstances the need to withhold is outweighed by other considerations which render it desirable, in the public interest, to make the information available.

2: Health information privacy rules

If an agency refuses to release information in response to an Official Information Act request it should give its reasons in appropriate terms relevant to that Act (eg: "I have decided to refuse the request under section 9(2)(a) of the Official Information Act to protect the privacy of the person concerned and I do not consider any other public interest consideration outweighs that interest in this case."). The Privacy Act should *not* be cited as the reason for refusing a request under the Official Information Act, even if privacy itself is the reason for withholding the information.

If information is released in good faith in response to a request under the Official Information Act, there is statutory protection against civil and criminal proceedings.

INFORMATION HELD AFTER DEATH

Information held by a health agency will continue to be covered by rule 11 for 20 years beyond the death of an individual (or until it is no longer kept by the agency). This is an acknowledgment that there can still be sensitivities associated with health information after a person has died. Note that all the exceptions in rule 11 will be available and it is not always necessary to gain authorisation from the representative. However, when a representative is available this person will usually be the appropriate person to authorise disclosure. The representative will normally be the executor or administrator of the estate (should one have been appointed) or the parent of a deceased child under 16.

See also rules 1, 3 and 6 and the Health Act 1956, sections 22C to 22H. The Evidence Act is discussed in Skegg and Paterson (ed), *Medical Law in New Zealand,* 2007. Refer to Privacy Act section 46(6), concerning the coverage of information about deceased persons.

Rule 12: UNIQUE IDENTIFIERS

(1) A health agency must not assign a unique identifier to an individual unless the assignment of that identifier is necessary to enable the health agency to carry out any 1 or more of its functions efficiently.

(2) A health agency must not assign to an individual a unique identifier that, to that agency's knowledge, has been assigned to that individual by another agency, unless—

(a) those 2 agencies are associated persons within the meaning of section OD 7 of the Income Tax Act 1994; or

(b) it is permitted by subrule (3) or (4).

(3) The following agencies may assign the same National Health Index number to an individual:

(a) any agency authorised expressly by statute or regulation; and

(b) any agency or class of agencies listed in Schedule 2.

(4) Notwithstanding subrule (2), any health agency may assign to a health practitioner, as a unique identifier, the registration number assigned to that individual by the relevant statutory registration body.

(5) A health agency that assigns unique identifiers to individuals must take all reasonable steps to ensure that unique identifiers are assigned only to individuals whose identity is clearly established.

(6) A health agency must not require an individual to disclose any unique identifier assigned to that individual unless the disclosure is for one of the purposes in connection with which that unique identifier was assigned or for a purpose that is directly related to one of those purposes.

(7) Subrules (1) to (5) do not apply in relation to the assignment of unique identifiers before the commencement of this code.

(8) Subrule (6) applies to any unique identifier, whether assigned before or after the commencement of this code.

Note: *An action is not a breach of this rule if it is authorised or required by or under law: Privacy Act 1993, section 7(4). Rule 12(2) was amended by Amendment No 3. Rule 12(3) was substituted by Amendment No 5. Rule 12(4) was substituted by Amendment No 6.*

2: Health information privacy rules

COMMENTARY

Section 2 of the Privacy Act defines unique identifier to mean an identifier: (a) that is assigned to an individual by an agency for the purposes of the operations of the agency; and (b) that uniquely identifies that individual in relation to that agency. To avoid doubt, section 2 makes it clear that the term does not include an individual's name.

The national unique identifier for health consumers is known as the National Health Index (or NHI) number. Rule 12 also applies to the unique identifiers assigned or demanded by health agencies, such as the identifier assigned by registration bodies to health practitioners.

The use of unique identifiers, in conjunction with other appropriate security practices, may help protect personal information when it is being transferred between providers (eg. from a hospital to a specialist or from a laboratory to a health professional). The use of a unique identifier allows a name and address to be removed from the transmission.

The reason for the controls in rule 12 is that widespread or improper use of unique identifiers may work against individual privacy. There is a risk that common numbering systems will facilitate the linking of databases and accumulation of medical information, which may be to the detriment of privacy if not controlled by the individuals concerned. A ubiquitous national unique identifier created for a specific purpose, such as the NHI can suffer from 'function creep' and evolve into a generic national identifier. Rule 12, and its equivalent principle in the Privacy Act, seek to prevent this by restricting the circumstances in which unique identifiers may be assigned and restricting the assigning of a unique identifier already assigned by another agency.

The word "assign" is not defined in the Code or the Privacy Act. It does not simply mean 'to create a new identifier'. The meaning generally preferred by the Office of the Privacy Commissioner, based on the definition of 'unique identifier' in the Privacy Act, is that 'assign' means to affix an identifier to an agency's records as the single or main identifier by which the assigning agency will refer to the individual. The unique identifier must be assigned for the purpose of the operations of the agency.

Rule 12 also prevents agencies from demanding that individuals disclose the unique identifier assigned to them by another agency – unless that is compatible with the purpose for which the unique identifier was first assigned. This restriction recognises that the presence of another agency's unique identifier on a computer system will allow searching by that identifier even if it is not the primary indexing reference.

The NHI number is widely used throughout the New Zealand health system. Its use outside of the health context is restricted and closely monitored.

Under subrule (3) the NHI number is exempted from the general prohibition on the assignment of unique identifiers by multiple agencies. Only health agencies listed in Schedule 2 may benefit from this exemption. This subrule ensures that the NHI number remains a unique identifier that is *specific* to the health sector, and can be used within the sector to improve health outcomes, but is not used to improperly link health information with other personal information.

See clause 3 and Schedule 2. A *Background Research Report on the National Health Index* is also available on the Office of the Privacy Commissioner's website at www.privacy.org.nz

6 CHARGES

(1) For the purposes of charging under section 35 of the Act in relation to information privacy requests concerning health information, a health agency that is not a public sector health agency must not require the payment, by or on behalf of any individual who wishes to make a request, of any charges in respect of a matter referred to in paragraphs 35(1)(a) to (f) of the Act except in accordance with this clause.

(2) Where an individual makes an information privacy request to a health agency that is not a public sector health agency, the agency may, unless prohibited by a law other than the Act or this code, make a reasonable charge,—

(a) where, on a particular day, that agency has made health information available to that individual in response to a request, for making the same or substantially the same health information available in accordance with any subsequent request within the period of 12 months after that day; or

(b) for providing a copy of an x-ray, a video recording, an MRI scan photograph, a PET scan photograph, or a CAT scan photograph.

(3) Where an agency intends to make a charge under subclause (2) and the amount of the charge is likely to exceed $30, the agency must provide the individual with an estimate of the charge before dealing with the request.

Note: *Clause 6(2)(b) was amended by Amendment No 6.*

COMMENTARY

Public sector agencies are prohibited from charging for access and correction requests by section 35 of the Privacy Act, set out in the appendix.

This clause provides additionally that non-public sector agencies are also prohibited from charging individuals for access or correction to their health information, except in the strictly limited circumstances set out in subclause (2).

In the limited circumstances where non-public sector agencies *are* permitted to charge, the charge must be reasonable and the requester must be provided with an estimate of the cost if it is likely to exceed $30.

It is important to note that the no-charging clause applies to requests by or on behalf of the individual concerned and not to third party requests for disclosure, even where the request is accompanied by a written consent by the individual to release the information.

The reference to x-rays etc in clause 6(2)(b) refers to the actual documents themselves and not to reports that are derived from them – the sole issue is the expense of duplication. The charges that can be made under clause 6(2) relate only to making information or copies available – not the decision to make information available or the other matters mentioned in section 35.

See sections 35 and 36 Privacy Act.

7 COMPLAINTS OF BREACH OF CODE

(1) Every health agency must designate a person or persons to deal with complaints alleging a breach of this code and facilitate the fair, simple, speedy, and efficient resolution of complaints.

(2) Every health agency to which this subclause applies must have a complaints procedure which provides that—

(a) when a complaint of breach of this code is received by the agency—

(i) the complaint is acknowledged in writing within 5 working days of receipt, unless it has been resolved to the satisfaction of the complainant within that period; and

(ii) the complainant is informed of any relevant internal and external complaints procedures; and

(iii) the complaint and the actions of the health agency regarding that complaint are documented; and

(b) within 10 working days of acknowledging the complaint, the agency must—

(i) decide whether it—

(A) accepts that the complaint is justified; or

(B) does not accept that the complaint is justified; or

(ii) if it decides that more time is needed to investigate the complaint, determine how much additional time is needed; and

(iii) if that additional time is more than 20 working days, inform the complainant of that determination and of the reasons for it; and

(c) as soon as practicable after a health agency decides whether or not it accepts that a complaint is justified, it must inform the individual of—

(i) the reasons for the decision; and

(ii) any actions the agency proposes to take; and

(iii) any appeal procedure the agency has in place; and

(iv) the right to complain to the Privacy Commissioner.

(3) Subclause (2) applies to any health agency specified in clause 4(2)(a), (c), (d), (e), (h), (i), (j), and (k) or the sixth and eighth item of Schedule 1.

(4) Nothing in this clause is to limit or restrict any provisions of Parts 4, 5, 8, or 9 of the Act or sections 55 to 57.

Note: *The original clauses 7 ("privacy officers") and 8 ("complaints of breach of code") were revoked by Amendments No 3 and 5 respectively. The present clause 7 was inserted by Amendment No 5.*

COMMENTARY

The Privacy Act:

- enables individuals to complain to the Privacy Commissioner if they believe their privacy has been infringed;
- provides that civil proceedings may be brought before the Human Rights Review Tribunal where complaints have not been resolved; and
- empowers the Tribunal to grant a range of remedies, such as declarations, damages, restraining orders and orders to take action to put things right.

Clause 7 requires:

- all health agencies to designate a person to deal with complaints; and
- most health agencies, including all health and disability service providers, to have internal complaints procedures that meet the standards and time limits set out in the clause.

PRIVACY OFFICERS

Section 23 of the Privacy Act places a responsibility on each health agency to ensure that there is, within that agency, at least one individual (referred to as a "privacy officer") whose responsibilities include:

- encouraging the agency to comply with the code;
- dealing with requests made to the agency under the Act and code;
- working with the Privacy Commissioner in relation to any investigations conducted under the Privacy Act in relation to that agency; and
- otherwise ensuring compliance by the health agency with the Act and the code.

The Privacy Act does not require the appointment of a person dedicated only to information privacy issues. It does require the responsibilities identified to be included in the duties of one or more persons within the agency. In the case of a single person health agency, that person would carry out the responsibilities of the privacy officer.

The Office of the Privacy Commissioner offers training opportunities for privacy officers.

COMPLAINTS PROCEDURES

Most health agencies will get complaints from time to time. It is important for purely business reasons, as well as privacy ones, that these be handled well. The way complaints are handled will depend in part on the size and function of the agency. For a larger agency, a formal process might be adopted involving a specially designated or independent person. Sometimes this will be the privacy officer. Sole health practitioners will usually have more informal and simple processes.

Any person may make a complaint directly to the Privacy Commissioner about an interference with his or her privacy (or complain on someone else's behalf). However, there are advantages for both the individual and the agency if the complainant first approaches the agency concerned and asks for the matter to be considered or reconsidered before complaining to the Commissioner. Clause 7 requires many health agencies to have internal complaints procedures. This is also a requirement of the Code of Health and Disability Services Consumers' Rights (clause 7(2) is, in general, modelled on the "Right to complain" in that code).

Elements of a good internal complaints procedure might include:

- a clear point of entry for complaints;
- having an independent person to review or determine the complaint;
- an opportunity for the complainant to properly air the grievance;
- expertise in handling complaints, which might be obtained from customer relations experience or training in dispute resolution; and
- responding to problems promptly.

Attention to good internal complaint handling procedures can be a useful and cost-effective way of resolving complaints without having them escalate externally to a costly and damaging degree.

If a health agency fails to comply with clause 7, it is deemed to have breached an information privacy principle (refer Privacy Act section 53(b)). If an agency's failure to comply with clause 7 causes some adverse consequence to an individual it may constitute an interference to privacy, for which the Act provides remedies (refer Privacy Act, section 66).

CLAUSE SUBJECT TO OTHER PARTS OF ACT

The clause does not affect the right to complain to the Privacy Commissioner and the provisions concerning the Commissioner and Human Rights Review Tribunal powers and processes are also unaffected. It is intended that effective internal complaints processes will result in the early resolution of grievances and diminish the need for individuals to resort to external agencies such as the Commissioner and the Tribunal.

The procedures and time limits set out in the clause do not apply to requests for access or correction. Requests of this nature are subject to the procedural provisions in Part 5 of the Privacy Act. If an access or correction request is refused, the requester may complain about the refusal to the agency and ask to have the complaint considered under the agency's internal complaints procedure. Alternatively, the requester may complain directly to the Privacy Commissioner.

See Part 8 of the Privacy Act. See also Code of Health and Disability Services Consumers' Rights, Right 10 ("Right to complain").

Schedules

SCHEDULE 1: SPECIFIED HEALTH AGENCIES

Ministry of Health

Health Research Council

New Zealand Council on Healthcare Standards

Institute of Environmental Science and Research Limited

The Interchurch Council on Hospital Chaplaincy

Health Benefits Limited

The Mental Health Commission

Accident Compensation Corporation

The Regulator under the Accident Insurance Act 1998 and the Injury Prevention, Rehabilitation and Compensation Act 2001

Note: *Schedule 1 was substituted by Amendment No 5 and amended by Amendment No 6.*

SCHEDULE 2: AGENCIES APPROVED TO ASSIGN NHI NUMBER

1 Ministry of Health

2 District Health Boards

3 Hospitals

4 Primary health organisations

5 Independent practitioner associations

6 Health practitioners

7 New Zealand Blood Service

8 Accident Compensation Corporation

9 Department of Corrections health services

10 New Zealand Defence Force health services

11 Pharmaceutical Management Agency of New Zealand

12 Any health agency which has a contract with the Accident Compensation Corporation or a District Health Board or the Ministry of Health to provide health or disability services.

Note: *Schedule 2 was substituted by Amendment No 6.*

COMMENTARY

Schedule 1 specifies certain agencies as being health agencies, in addition to the agencies outlined in clause 3 and subclause 4(2).

Schedule 2 sets out the list of agencies permitted to assign the NHI number as a unique identifier, in accordance with rule 12(3)(b). Agencies may also be expressly authorised by statute or regulation to assign the NHI number (rule 12(3)(a)). See the commentary to rule 12 on page 72 for a discussion of “assign”.

Appendix EXTRACTS FROM ENACTMENTS

Extracts are reprinted from the following statutes and regulations:

The reprinted extracts are believed to be correct as at December 2008. However, it is prudent, if proposing to rely on a provision in a law, to check with an official published version of the statute book to check for errors, amendments and repeals.

Extracts from Privacy Act 1993

Note: *To assist users of the code certain subsections, not of relevance in the health sector, have been omitted. Where reference is made to a particular principle, the corresponding rule in the code is shown in square brackets. For example "principle 6" is shown as "[rule 6]". Similar reference to clause 6 of the code is substituted in sections 35 and 40.*

2 INTERPRETATION

(1) In this Act, unless the context otherwise requires,—

action includes failure to act; and also includes any policy or practice:

agency—

(a) means any person or body of persons, whether corporate or unincorporate, and whether in the public sector or the private sector; and, for the avoidance of doubt, includes a Department; but

(b) does not include—

(i) the Sovereign; or

(ii) the Governor-General or the Administrator of the Government; or

(iii) the House of Representatives; or

(iv) a member of Parliament in his or her official capacity; or

(v) the Parliamentary Service Commission; or

(vi) the Parliamentary Service, except in relation to personal information about any employee or former employee of that agency in his or her capacity as such an employee; or

(vii) in relation to its judicial functions, a court; or

(viii) in relation to its judicial functions, a tribunal, or

(ix) an Ombudsman; or

(x) a Royal Commission; or

(xi) a commission of inquiry appointed by an Order in Council made under the Commissions of Inquiry Act 1908; or

(xii) a commission of inquiry or board of inquiry or court of inquiry or committee of inquiry appointed, pursuant to, and not by, any provision of an Act, to inquire into a specified matter; or

(xiii) in relation to its news activities, any news medium:

collect does not include receipt of unsolicited information:

Commissioner means the Privacy Commissioner appointed under section 12:

correct, in relation to personal information, means to alter that information by way of **correction,** deletion, or addition; and correction has a corresponding meaning:

document means a document in any form; and includes—

(a) any writing on any material:

(b) any information recorded or stored by means of any tape-recorder, computer, or other device; and any material subsequently derived from information so recorded or stored:

(c) any label, marking, or other writing that identifies or describes any thing of which it forms part, or to which it is attached by any means:

(d) any book, map, plan, graph, or drawing:

(e) any photograph, film, negative, tape, or other device in which one or more visual images are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced:

individual means a natural person, other than a deceased natural person:

individual concerned, in relation to personal information, means the individual to whom the information relates:

information privacy request has the meaning given to it by section 33:

news activity means—

(a) the gathering of news, or the preparation or compiling of articles or programmes of or concerning news, observations on news, or current affairs, for the purposes of dissemination to the public or any section of the public:

(b) the dissemination, to the public or any section of the public, of any article or programme of or concerning—

(i) news:

(ii) observations on news:

(iii) current affairs:

news medium means any agency whose business, or part of whose business, consists of a news activity; but, in relation to principles 6 and 7, does not include Radio New Zealand Limited or Television New Zealand Limited:

publicly available information means personal information that is contained in a publicly available publication:

unique identifier means an identifier—

(a) that is assigned to an individual by an agency for the purposes of the operations of the agency; and

(b) that uniquely identifies that individual in relation to that agency;—

but, for the avoidance of doubt, does not include an individual's name used to identify that individual:

working day means any day of the week other than—

(a) Saturday, Sunday, Good Friday, Easter Monday, Anzac Day, Labour Day, the Sovereign's birthday, and Waitangi Day; and

(b) a day in the period commencing with the 25th day of December in any year and ending with the 15th day of January in the following year.

3 INFORMATION HELD BY AGENCY

(1) Subject to subsection (2), information that is held by an officer or employee or member of an agency in that person's capacity as such an officer or employee or member or in that person's capacity as a statutory officer shall be deemed, for the purposes of this Act, to be held by the agency of which that person is an officer or employee or member.

(2) Nothing in subsection (1) applies in respect of any information that any officer or employee or member of a public sector agency would not hold but for that person's membership of, or connection with, a body other than a public sector agency, except where that membership or connection is in that person's capacity as an officer or an employee or a member of that public sector agency or as a statutory officer.

(3) Nothing in subsection (1) applies in respect of any information that any officer or employee or member of any agency (not being a public sector agency) would not hold but for that person's membership of, or connection with, any other agency, except where that membership or connection is in that person's capacity as an officer or an employee or a member of that first-mentioned agency.

(4) For the purposes of this Act, where an agency holds information—

(a) solely as agent; or

(b) for the sole purpose of safe custody; or

(c) for the sole purpose of processing the information on behalf of another agency,—

and does not use or disclose the information for its own purposes, the information shall be deemed to be held by the agency on whose behalf that information is so held or, as the case may be, is so processed.

4 ACTIONS OF, AND DISCLOSURE OF INFORMATION TO, STAFF OF AGENCY, ETC

For the purposes of this Act, an action done by, or information disclosed to, a person employed by, or in the service of, an agency in the performance of the duties of the person's employment shall be treated as having been done by, or disclosed to, the agency.

7 SAVINGS

(1) Nothing in [rule 6] or [rule 11] derogates from any provision that is contained in any enactment and that authorises or requires personal information to be made available.

(2) Nothing in [rule 6] or [rule 11] derogates from any provision that is contained in any other Act of Parliament and that—

(a) imposes a prohibition or restriction in relation to the availability of personal information; or

(b) regulates the manner in which personal information may be obtained or made available.

(3) Nothing in [rule 6] or [rule 11] derogates from any provision—

(a) that is contained in any regulations within the meaning of the Regulations (Disallowance)

Act 1989 made by Order in Council and in force—

(i) in so far as those [rules] apply to a Department, a Minister, an organisation, or a public sector agency (as defined in paragraph (b) of the definition of that term in section 2(1)) that is established for the purposes of assisting or advising, or performing functions connected with, a Department, a Minister, or an organisation, immediately before the 1st day of July 1983; and

(ii) in so far as those [rules] apply to a local authority or a public sector agency (as so defined) that is established for the purposes of assisting or advising, or performing functions connected with, a local authority, immediately before the 1st day of March 1988; and

(iii) in so far as those [rules] apply to any other agency, immediately before the 1st day of July 1993; and

(b) that—

(i) imposes a prohibition or restriction in relation to the availability of personal information; or

(ii) regulates the manner in which personal information may be obtained or made available.

(4) An action is not a breach of any of [rules 1 to 5, 7 to 10, and 12] if that action is authorised or required by or under law.

(5) [omitted].

(6) Subject to the provisions of Part 7 of the Act, nothing in any of the [health information privacy rules] shall apply in respect of a public register.

PART 4: GOOD REASONS FOR REFUSING ACCESS TO PERSONAL INFORMATION

Note: *Section 27(2), concerning international relations, and section 29(1)(g), concerning information held by Radio NZ and TVNZ, have been omitted as being of little relevance to users of the code.*

27 SECURITY, DEFENCE, INTERNATIONAL RELATIONS, ETC

(1) An agency may refuse to disclose any information requested pursuant to [rule 6] if the disclosure of the information would be likely—

(a) to prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand; or

(b) to prejudice the entrusting of information to the Government of New Zealand on a basis of confidence by—

(i) the government of any other country or any agency of such a government;

(ii) any international organisation; or

(c) to prejudice the maintenance of the law, including the prevention, investigation, and detection of offences, and the right to a fair trial; or

(d) to endanger the safety of any individual.

(2) [omitted]

28 TRADE SECRETS

(1) Subject to subsection (2), an agency may refuse to disclose any information requested pursuant to [rule 6] if the withholding of the information is necessary to protect information where the making available of the information—

(a) would disclose a trade secret; or

(b) would be likely unreasonably to prejudice the commercial position of the person who supplied or who is the subject of the information.

(2) Information may not be withheld under subsection (1) if, in the circumstances of the particular case, the withholding of that information is outweighed by other considerations which render it desirable, in the public interest, to make the information available.

29 OTHER REASONS FOR REFUSAL OF REQUESTS

(1) An agency may refuse to disclose any information requested pursuant to [rule 6] if—

(a) the disclosure of the information would involve the unwarranted disclosure of the affairs of another individual or of a deceased individual; or

(b) the disclosure of the information or of information identifying the person who supplied it, being evaluative material, would breach an express or implied promise—

(i) which was made to the person who supplied the information; and

(ii) which was to the effect that the information or the identity of the person who supplied it or both would be held in confidence; or

(c) after consultation undertaken (where practicable) by or on behalf of the agency with an individual's medical practitioner, the agency is satisfied that—

(i) the information relates to that individual; and

(ii) the disclosure of the information (being information that 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; or

(d) in the case of an individual under the age of 16, the disclosure of that information would be contrary to that individual's interests; or

(e) the disclosure of that information (being information in respect of an individual who has been convicted of an offence or is or has been detained in custody) would be likely to prejudice the safe custody or the rehabilitation of that individual; or

(f) the disclosure of the information would breach legal professional privilege; or

(g) [omitted]

(h) the disclosure of the information, being information contained in material placed in any library or museum or archive, would breach a condition subject to which that material was so placed; or

(i) the disclosure of the information would constitute contempt of Court or of the House of Representatives; or

(j) the request is frivolous or vexatious, or the information requested is trivial.

(2) An agency may refuse a request made pursuant to [rule 6] if—

(a) the information requested is not readily retrievable; or

(b) the information requested does not exist or cannot be found; or

(c) the information requested is not held by the agency and the person dealing with the request has no grounds for believing that the information is either—

(i) held by another agency; or

(ii) connected more closely with the functions or activities of another agency.

(3) For the purposes of subsection (1)(b), the term "evaluative material" means evaluative or opinion material compiled solely—

(a) for the purpose of determining the suitability, eligibility, or qualifications of the individual to whom the material relates—

(i) for employment or for appointment to office; or

(ii) for promotion in employment or office or for continuance in employment or office; or

(iii) for removal from employment or office; or

(iv) for the awarding of contracts, awards, scholarships, honours, or other benefits; or

(b) for the purpose of determining whether any contract, award, scholarship, honour, or benefit should be continued, modified, or cancelled; or

(c) for the purpose of deciding whether to insure any individual or property or to continue or renew the insurance of any individual or property.

30 REFUSAL NOT PERMITTED FOR ANY OTHER REASON

Subject to sections 7, 31, and 32, no reasons other than one or more of the reasons set out in sections 27 to 29 justifies a refusal to disclose any information requested pursuant to [rule 6].

32 INFORMATION CONCERNING EXISTENCE OF CERTAIN INFORMATION

Where a request made pursuant to [rule 6] relates to information to which section 27 or section 28 applies, or would, if it existed, apply, the agency dealing with the request may, if it is satisfied that the interest protected by section 27 or section 28 would be likely to be prejudiced by the disclosure of the existence or non-existence of that information, give notice in writing to the applicant that it neither confirms nor denies the existence or non-existence of that information.

PART 5: PROCEDURAL PROVISIONS RELATING TO ACCESS TO AND CORRECTION OF PERSONAL INFORMATION

33 APPLICATION

This Part applies to the following requests (in this Act referred to as information privacy requests):

(a) a request made pursuant to [rule 6(1)(a)] to obtain confirmation of whether or not an agency holds personal information:

(b) a request made pursuant to [rule 6(1)(b)] to be given access to personal information:

(c) a request made pursuant [subrule 7(1)] for correction of personal information.

34 WHO MAY MAKE REQUESTS

An information privacy request may be made only by an individual who is—

(a) a New Zealand citizen; or

(b) a permanent resident of New Zealand; or

(c) an individual who is in New Zealand.

35 CHARGES

(1) Subject to section 36, a public sector agency shall not require the payment, by or on behalf of any individual who wishes to make an information privacy request, of any charge in respect of—

(a) the provision of assistance in accordance with section 38; or

(b) the making of the request to that agency; or

(c) the transfer of the request to any other agency; or

(d) the processing of the request, including deciding whether or not the request is to be granted and, if so, in what manner; or

(e) the making available of information in compliance, in whole or in part, with the request; or

(f) in the case of a request made pursuant to [subrule 7(1)]—

(i) the correction of any information in compliance, in whole or in part, with the request; or

(ii) the attaching, to any information, of a statement of any correction sought but not made.

(2) Subject to subsection (4), an agency that is not a public sector agency shall not require the payment, by or on behalf of any individual who wishes to make an information privacy request, of any charge in respect of—

(a) the provision of assistance in accordance with section 38; or

(b) the making of the request to that agency; or

(c) the transfer of the request to any other agency; or

(d) the processing of the request, including deciding whether or not the request is to be granted and, if so, in what manner.

(3) [omitted]

(4) [omitted]

(5) Any charge fixed by an agency pursuant to [clause 6 of the code] or pursuant to an authority granted pursuant to section 36 in respect of an information privacy request shall be reasonable, and (in the case of a charge fixed in respect of the making available of information) regard may be had to the cost of the labour and materials involved in making information available in accordance with the request and to any costs incurred pursuant to a request of the applicant for the request to be treated as urgent.

(6) The provisions of subsection (3) to (5), in so far as they relate to the fixing, by any agency that is not a public sector agency, of any charge in respect of any information privacy request, shall apply subject to any provisions to the contrary in any code of practice issued under section 46 and for the time being in force.

36 COMMISSIONER MAY AUTHORISE PUBLIC SECTOR AGENCY TO CHARGE

(1) Where a public sector agency satisfies the Commissioner that the agency is commercially disadvantaged, in comparison with any competitor in the private sector, by reason that the agency is prevented, by subsection (1) of section 35, from imposing a charge in respect of any of the matters referred to in paragraph (e) or paragraph (f) of that subsection, the Commissioner may authorise that agency to impose a charge in respect of either or both of those matters.

(2) The Commissioner may impose in respect of any authority granted pursuant to subsection (1) such conditions as the Commissioner thinks fit.

(3) The Commissioner may, at any time, revoke any authority granted to an agency pursuant to subsection (1), but shall not revoke any such authority without giving the agency an opportunity to be heard.

37 URGENCY

If an individual making an information privacy request asks that his or her request be treated as urgent, that individual shall give his or her reasons why the request should be treated as urgent.

38 ASSISTANCE

It is the duty of every agency to give reasonable assistance to an individual, who—

(a) wishes to make an information privacy request; or

(b) in making such a request, has not made the request in accordance with the requirements of this Act; or

(c) has not made his or her request to the appropriate agency,—

to make a request in a manner that is in accordance with the requirements of this Act or to direct his or her request to the appropriate agency.

39 TRANSFER OF REQUESTS

Where—

(a) an information privacy request is made to an agency or is transferred to an agency in accordance with this section; and

(b) the information to which the request relates—

(i) is not held by the agency but is believed by the person dealing with the request to be held by another agency; or

(ii) is believed by the person dealing with the request to be more closely connected with the functions or activities of another agency,—

the agency to which the request is made shall promptly, and in any case not later than 10 working days after the day on which the request is received, transfer the request to the other agency and inform the individual making the request accordingly.

40 DECISIONS ON REQUESTS

(1) Subject to this Act, the agency to which an information privacy request is made or transferred in accordance with this Act shall, as soon as reasonably practicable, and in any case not later than 20 working days after the day on which the request is received by that agency,—

(a) decide whether the request is to be granted and, if it is to be granted, in what manner and, subject to [clause 6 of the code], for what charge (if any); and

(b) give or post to the individual who made the request notice of the decision on the request.

(2) Where any charge is imposed, the agency may require the whole or part of the charge to be paid in advance.

(3) Where an information privacy request is made or transferred to a Department, the decision on that request shall be made by the chief executive of that Department or an officer or employee of that Department authorised by that chief executive, unless that request is transferred in accordance with section 39 of this Act to another agency.

(4) Nothing in subsection (3) prevents the chief executive of a Department or any officer or employee of a Department from consulting a Minister or any other person in relation to the decision that the chief executive or officer or employee proposes to make on any information privacy request made or transferred to the Department in accordance with this Act.

41 EXTENSION OF TIME LIMITS

(1) Where an information privacy request is made or transferred to an agency, the agency may extend the time limit set out in section 39 or section 40 (1) in respect of the request if—

(a) the request is for a large quantity of information or necessitates a search through a large quantity of information, and meeting the original time limit would unreasonably interfere with the operations of the agency; or

(b) consultations necessary to make a decision on the request are such that a proper response to the request cannot reasonably be made within the original time limit.

(2) Any extension under subsection (1) shall be for a reasonable period of time having regard to the circumstances.

(3) The extension shall be effected by giving or posting notice of the extension to the individual who made the request within 20 working days after the day on which the request is received.

(4) The notice effecting the extension shall—

(a) specify the period of the extension; and

(b) give the reasons for the extension; and

(c) state that the individual who made the request for the information has the right, under section 67, to make a complaint to the Commissioner about the extension; and

(d) contain such other information as is necessary.

42 DOCUMENTS

(1) Where the information in respect of which an information privacy request is made by any individual is comprised in a document, that information may be made available in one or more of the following ways:

(a) by giving the individual a reasonable opportunity to inspect the document; or

(b) by providing the individual with a copy of the document; or

(c) in the case of a document that is an article or thing from which sounds or visual images are capable of being reproduced, by making arrangements for the individual to hear or view those sounds or visual images; or

(d) in the case of a document by which words are recorded in a manner in which they are capable of being reproduced in the form of sound or in which words are contained in the form of shorthand writing or in codified form, by providing the individual with a written transcript of the words recorded or contained in the document; or

(e) by giving an excerpt or summary of the contents; or

(f) by furnishing oral information about its contents.

(2) Subject to section 43, the agency shall make the information available in the way preferred by the individual requesting it unless to do so would—

(a) impair efficient administration; or

(b) be contrary to any legal duty of the agency in respect of the document; or

(c) prejudice the interests protected by section 27 or section 28 or section 29 and (in the case of the interests protected by section 28) there is no countervailing public interest.

(3) Where the information is not provided in the way preferred by the individual requesting it, the agency shall, subject to section 32, give to that individual—

(a) the reason for not providing the information in that way; and

(b) if that individual so requests, the grounds in support of that reason, unless the giving of those grounds would itself prejudice the interests protection by section 27 or section 28 or section 29 and (in the case of the interests protected by section 28) there is no countervailing public interest.

43 DELETION OF INFORMATION FROM DOCUMENTS

(1) Where the information in respect of which an information privacy request is made is comprised in a document and there is good reason for withholding some of the information contained in that document, the other information in that document may be made available by making a copy of that document available with such deletions or alterations as are necessary.

(2) Where a copy of a document is made available under subsection (1), section, the agency shall, subject to section 32, give to the individual—

(a) the reason for withholding the information; and

(b) if the individual so requests, the grounds in support of that reason, unless the giving of those grounds would itself prejudice the interests protected by section 27 or section 28 or section 29 and (in the case of the interests protected by section 28) there is no countervailing public interest.

44 REASON FOR REFUSAL TO BE GIVEN

Where an information privacy request made by an individual is refused, the agency shall,—

(a) subject to section 32, give to the individual—

(i) the reason for its refusal; and

(ii) if the individual so requests, the grounds in support of that reason, unless the giving of those grounds would itself prejudice the interests protection by section 27 or section 28 or section 29 and (in the case of the interests protected by section 28) there is no countervailing public interest; and

(b) give to the individual information concerning the individual's right, by way of complaint under section 67 to the Commissioner, to seek an investigation and review of the refusal.

45 PRECAUTIONS

Where an information privacy request is made pursuant to [rule 6(1)(b)], the agency—

(a) shall not give access to that information unless it is satisfied concerning the identity of the individual making the request; and

(b) shall ensure, by the adoption of appropriate procedures, that any information intended for an individual is received—

(i) only by that individual; or

(ii) where the request is made by an agent of the individual, only by that individual or his or her agent; and

(c) shall ensure that, where the request is made by an agent of the individual, the agent has the written authority of that individual to obtain the information or is otherwise properly authorised by that individual to obtain the information.

54 COMMISSIONER MAY AUTHORISE COLLECTION, USE OR DISCLOSURE OF PERSONAL INFORMATION

(1) The Commissioner may authorise an agency to collect, use or disclose personal information, even though that collection, use, or disclosure would otherwise be in breach of [rule 2 or 10 or 11], if the Commissioner is satisfied that, in the special circumstances of the case,—

(a) the public interest in that collection or, as the case requires, that use or that disclosure outweighs, to a substantial degree, any interference with the privacy of the individual that could result from that collection or, as the case requires, that use or that disclosure; or

(b) that collection or, as the case requires, that use or that disclosure involves a clear benefit to the individual concerned that outweighs any interference with the privacy of the individual that could result from that collection or, as the case requires, that use or that disclosure.

(2) The Commissioner may impose in respect of any authority granted under subsection (1) such conditions as the Commissioner thinks fit.

(3) The Commissioner shall not grant an authority under subsection (1) in respect of the collection, use, or disclosure of any personal information for any purpose if the individual concerned has refused to authorise the collection or, as the case requires, the use or disclosure of the information for that purpose.

126 LIABILITY OF EMPLOYER AND PRINCIPALS

(1) Subject to subsection (4), anything done or omitted by a person as the employee of another person shall, for the purposes of this Act, be treated as done or omitted by that other person as well as by the first-mentioned person, whether or not it was done with that other person's knowledge or approval.

(2) Anything done or omitted by a person as the agent of another person shall, for the purposes of this Act, be treated as done or omitted by that other person as well as by the first-mentioned person, unless it is done or omitted without that other person's express or implied authority, precedent or subsequent.

(3) Anything done or omitted by a person as a member of any agency shall, for the purposes of this Act, be treated as done or omitted by that agency as well as by the first-mentioned person, unless it is done or omitted without that agency's express or implied authority, precedent or subsequent.

(4) In proceedings under this Act against any person in respect of an act alleged to have been done by an employee of that person, it shall be a defence for that person to prove that he or she or it took such steps as were reasonably practicable to prevent the employee from doing that act, or from doing as an employee of that person acts of that description.

Extract from Children, Young Persons, and their Families Act 1989

15 REPORTING OF ILL-TREATMENT OR NEGLECT OF CHILD OR YOUNG PERSON

Any person who believes that any child or young person has been, or is likely to be, harmed (whether physically, emotionally, or sexually), ill-treated, abused, neglected, or deprived may report the matter to a Social Worker or a member of the Police.

16 PROTECTION OF PERSON REPORTING ILL-TREATMENT OR NEGLECT OF CHILD OR YOUNG PERSON

No civil, criminal, or disciplinary proceedings shall lie against any person in respect of the disclosure or supply, or the manner of the disclosure or supply, by that person pursuant to section 15 of information concerning a child or young person (whether or not that information also concerns any other person), unless the information was disclosed or supplied in bad faith.

Extract from Evidence Act 2006

59 PRIVILEGE IN CRIMINAL PROCEEDINGS FOR INFORMATION OBTAINED BY MEDICAL PRACTITIONERS AND CLINICAL PSYCHOLOGISTS

(1) This section—

(a) applies to a person who consults or is examined by a medical practitioner or a clinical psychologist for drug dependency or any other condition or behaviour that may manifest itself in criminal conduct; but

(b) does not apply in the case of a person who has been required by an order of a Judge, or by other lawful authority, to submit himself or herself to the medical practitioner or clinical psychologist for any examination, test, or for any other purpose.

(2) A person has a privilege in a criminal proceeding in respect of any communication made by the person to a medical practitioner or clinical psychologist that the person believes is necessary to enable the medical practitioner or clinical psychologist to examine, treat, or care for the person for drug dependency or any other condition or behaviour that may manifest itself in criminal conduct.

(3) A person has a privilege in a criminal proceeding in respect of information obtained by a medical practitioner or clinical psychologist as a result of consulting with or examining the person to enable the medical practitioner or clinical psychologist to examine, treat, or care for the person for drug dependency or any other condition or behaviour that may manifest itself in criminal conduct.

(4) A person has a privilege in a criminal proceeding in respect of information consisting of a prescription, or notes of a prescription, for treatment prescribed by a medical practitioner or clinical psychologist as a result of consulting with or examining the person to enable the medical practitioner or clinical psychologist to treat or care for the person for drug dependency or any other condition or behaviour that may manifest itself in criminal conduct.

(5) A reference in this section to a communication to or information obtained by a medical practitioner or a clinical psychologist is to be taken to include a reference to a communication to or information obtained by a person acting in a professional capacity on behalf of a medical practitioner or clinical psychologist in the course of the examination or treatment of, or care for, the person by that medical practitioner or clinical psychologist.

(6) In this section,—

clinical psychologist means a health practitioner—

(a) who is, or is deemed to be, registered with the Psychologists Board continued by section 114(1)(a) of the Health Practitioners Competence Assurance Act 2003 as a practitioner of the profession of psychology; and

(b) who is by his or her scope of practice permitted to diagnose and treat persons suffering from mental and emotional problems

drug dependency means the state of periodic or chronic intoxication produced by the repeated consumption, smoking, or other use of a controlled drug (as defined in section 2(1) of the Misuse of Drugs Act 1975) detrimental to the user, and involving a compulsive desire to continue consuming, smoking, or otherwise using the drug or a tendency to increase the dose of the drug.

Extracts from Health Act 1956

22C DISCLOSURE OF HEALTH INFORMATION

(1) Any person (being an agency that provides services or arranges the provision of services) may disclose health information—

(a) If that information—

(i) is required by any person specified in subsection (2); and

(ii) is required (or, in case of the purpose set out in paragraph (j) of that subsection, is essential) for the purpose set out in that subsection in relation to the person so specified; or

(b) if that disclosure is permitted—

(i) by or under a code of practice issued under section 46 of the Privacy Act 1993; or

(ii) if no such code of practice applies in relation to the information, by any of the information privacy principles set out in section 6 of that Act.

(2) The persons and purposes referred to in subsection (1)(a) are as follows:

(a) any medical officer of a prison within the meaning of the Corrections Act 2004, for the purposes of exercising or performing any of that person's powers, duties, or functions under that Act:

(b) any probation officer within the meaning of the Corrections Act 2004, for the purposes of exercising or performing any of that person's powers, duties, or functions under any enactment:

(c) a Social Worker or a Care and Protection Co-ordinator within the meaning of the Children, Young Persons, and Their Families Act 1989, for the purposes of exercising or performing any of that person's powers, duties, or functions under that Act:

(d) any employee of the department for the time being responsible for the administration of the Social Security Act, for the purposes of administering section 75 of the Social Security Act 1964:

(e) any member of the New Zealand Defence Force, for the purposes of administering the Armed Forces Discipline Act 1971 or the Defence Act 1990:

(f) any member of the Police, for the purposes of exercising or performing any of that person's powers, duties or functions:

(g) any employee of the Ministry of Health, for the purposes of—

(i) administering this Act or the Hospitals Act 1957; or

(ii) compiling statistics for health purposes:

(h) any employee of the Ministry of Agriculture and Forestry authorised by the chief executive of that Ministry to receive the information, for the purposes of administering the Meat Act 1981 or the Animal Products Act 1999;

(i) any employee of the Land Transport New Zealand, for statistical or research purposes in relation to road safety or the environment:

(j) any employee of a District Health Board, for the purposes of exercising or performing any of that Board's powers, duties, or functions under the New Zealand Public Health and Disability Act 2000.

(3) For the purposes of principle 11(d) of the Privacy Act 1993, the disclosure of health information about an individual may be authorised—

(a) by that individual personally, if he or she has attained the age of 16 years; or

(b) by a representative of that individual.

22D DUTY TO PROVIDE HEALTH INFORMATION

(1) The Minister may at any time, by notice in writing, require any District Health Board to provide, in such manner as may from time to time be required, such returns or other information as is specified in the notice concerning the condition or treatment of, or the services provided to, any individuals in order to obtain statistics for health purposes or for the purposes of advancing health knowledge, health education, or health research.

(2) Subject to subsection (3), it is the duty of a District Health Board to provide the returns or other information specified in a notice given to it under subsection (1) within such time, and in such form, as is specified in the notice.

(3) No information that would enable the identification of an individual may be provided under this section unless—

(a) the individual consents to the provision of such information; or

(b) the identifying information is essential for the purposes for which the information is sought.

(4) For the purposes of subsection (3)(a), consent to the provision of information may be given—

(a) by the individual personally, if he or she has attained the age of 16 years; or

(b) by a representative of that individual.

22F COMMUNICATION OF INFORMATION FOR DIAGNOSTIC AND OTHER PURPOSES

(1) Every person who holds health information of any kind shall, at the request of the individual about whom the information is held, or a representative of that individual, or any other person that is providing, or is to provide, services to that individual, disclose that information to that individual or, as the case requires, to that representative or to that other person.

(2) A person that holds health information may refuse to disclose that information under this section if—

(a) that person has a lawful excuse for not disclosing that information; or

(b) where the information is requested by someone other than the individual about whom it is held (not being a representative of that individual), the holder of the information has reasonable grounds for believing that individual does not wish the information to be disclosed; or

(c) refusal is authorised by a code of practice issued under section 46 of the Privacy Act 1993.

(3) For the purposes of subsection (2)(a), neither—

(a) the fact that any payment due to the holder of any information or to any other person has not been made; nor

(b) the need to avoid prejudice to the commercial position of the holder of any information or of any other person; nor

(c) the fact that disclosure is not permitted under any of the information privacy principles set out in section 6 of the Privacy Act 1993—

shall constitute a lawful excuse for not disclosing information under this section.

(4) Where any person refuses to disclose health information in response to a request made under this section, the person whose request is refused may make a complaint to the Privacy Commissioner under Part 7 of the Privacy Act 1993, and that Part of the Act, so far as applicable and with all necessary modifications, shall apply in relation to that complaint as if the refusal to which the complaint relates were a refusal to make information available in response to an information privacy request within the meaning of that Act.

(5) Nothing in subsection (4) limits any other remedy that is available to any person who is aggrieved by any refusal to disclose information under this section.

22G INSPECTION OF RECORDS

(1) In this section, **provider** means a person who has claimed payment for services from 1 or more of the following:

(a) the Ministry of Health:

(b) a district health board:

(c) the Health Funding Authority or a person authorised by the Health Funding Authority to make payments:

(d) a regional health authority or a person authorised by a regional health authority to make payments:

(e) a hospital and health service:

(f) a Crown health enterprise:

(g) an area health board:

(h) a hospital board:

(i) the Department of Health.

(2) Every provider must, forthwith after a request by the Director-General or the chief executive of a district health board or of Health Benefits Limited, make available any records of the provider that relate to the services concerned for inspection—

(a) by a person authorised in writing by the Director-General or the chief executive of the district health board or Health Benefits Limited (as the case may be) for this purpose, being a person who holds a professional qualification relevant to the services provided by the provider or any other person the Director-General or the chief executive considers appropriate; and

(b) for the purposes of verifying the claim for payment.

(3) Any person authorised in accordance with subsection (2) to inspect the records of a provider may copy or take notes of those records for the purposes of the inspection.

22H ANONYMOUS HEALTH INFORMATION

Notwithstanding any enactment, rule of law, or other obligation, any person may supply to any other person health information that does not enable the identification of the individual to whom the information relates.

Extract from Health Retention of Health (Information) Regulations 1996

3 GENERAL EFFECT

(1) The general effect of these regulations is to impose an obligation on providers of … services to retain, for a minimum period, health information relating to identifiable individuals.

(2) That obligation is imposed on the provider that for the time being holds the health information, even though the information may have been transferred to that provider.

5 DEFINITION OF "MINIMUM RETENTION PERIOD"

In these regulations, unless the context otherwise requires, "minimum retention period", in relation to health information that relates to an identifiable individual, means a period of 10 years beginning on the day after the date shown in the health information as the most recent date on which a provider provided services, to that individual.

6 HEALTH INFORMATION TO BE KEPT FOR MINIMUM RETENTION PERIOD

(1) Subject to subclause (2) of this regulation and to regulations 7, 8, and 9 of these regulations, every provider that holds health information shall retain that health information for the minimum retention period.

(2) Subclause (1) of this regulation does not prevent a provider from transferring health information that relates to an identifiable individual to,—

(a) another provider; or

(b) the individual to whom the information relates; or

(c) if that individual is dead, the personal representative of that individual.

11 OFFENCE

(1) Every provider commits an offence who fails, without reasonable excuse, to comply with regulation 6(1) of these regulations.

(2) Every provider who commits an offence against subclause (1) of this regulation is liable on summary conviction to a fine not exceeding $500.

Extract from Medicines Act 1981

49A STATEMENTS REGARDING PERSONS DEPENDENT ON PRESCRIPTION MEDICINES OR RESTRICTED MEDICINES

(1) If a Medical Officer of Health has reason to believe that any person is or is likely to become dependent on any prescription medicine or restricted medicine, the Medical Officer of Health may, for the purpose of preventing or restricting the supply of prescription medicines or restricted medicines to that person, or of assisting in the cure or mitigation or avoidance of the dependence of that person, publish statements relating to that person to all or any of the members of all or any of the classes of persons set out in subsection (3).

(2) Every statement made under subsection (1) shall be privileged unless the publication is proved to be made with malice.

(3) The classes of person referred to in subsection (1) are as follows:

(a) officers:

(b) officers and employees of any district health board established by or under section 19 of the New Zealand Public Health and Disability Act 2000:

(c) people providing, or employed in providing hospital care (within the meaning of the Health and Disability Services (Safety) Act 2001):

(d) Managers of prisons within the meaning of the Corrections Act 2004:

(e) managers and superintendents of institutions within the meaning of the Alcoholism and Drug Addiction Act 1966:

(f) medical practitioners:

(g) dentists:

(ga) registered midwives:

(gb) designated prescribers:

(h) members of the Police:

(i) persons who deal in prescription medicines or restricted medicines in the course of business.

(4) Nothing in subsection (1) or subsection (2) shall limit or affect any right or duty that a Medical Officer of Health may otherwise possess to publish a statement to any person.

(5) Every person commits an offence against this Act who, except in the course of duty as a member of a class set out in subsection (3) or as an officer or servant of the Crown, publishes any information obtained, whether by that person or any other person, from a statement made pursuant to subsection (1), or any comment on any such statement.

Extract from Misuse of Drugs Act 1975

20 STATEMENTS REGARDING DRUG DEPENDENT PERSONS

(1) If a Medical Officer of Health has reason to believe that any person is or is likely to become dependent on any controlled drug, he may, for the purpose of preventing or restricting the supply of the controlled drugs to that person, or of assisting in the cure or mitigation or avoidance of the dependence of that person, publish statements relating to that person to all or any of the members of all or any of the classes of persons set out in subsection (3).

(2) Every statement made under subsection (1) shall be privileged unless the publication is proved to be made with malice.

(3) The classes of persons referred to in subsection (1) are as follows:

(a) employees of any district health board established by or under the New Zealand Public Health and Disability Act 2000:

(b) a hospital care operator within the meaning of section 8(4) of the Health and Disability Services (Safety) Act 2001:

(c) managers of prisons within the meaning of the Corrections Act 2004:

(d) managers and superintendents of institutions within the meaning of the Alcoholism and Drug Addiction Act 1966:

(e) medical practitioners:

(f) dentists:

(fa) registered midwives:

(fb) designated prescribers:

(g) members of the Police:

(h) persons who deal in controlled drugs in the course of business.

(4) Nothing in subsection (1) or subsection (2) shall limit or affect any right or duty which a Medical Officer of Health may otherwise possess to publish a statement to any person.

(5) Every person commits an offence against this Act who, except in the course of duty as a member of a class set out in subsection (3) or as an officer or servant of the Crown, publishes any information obtained, whether by him or any other person, from a statement made pursuant to subsection (1), or any comment on any such statement.

Extracts from New Zealand Bill of Rights Act 1990

10 RIGHT NOT TO BE SUBJECTED TO MEDICAL ... EXPERIMENTATION

Every person has the right not to be subjected to medical ... experimentation without that person's consent.

11 RIGHT TO REFUSE TO UNDERGO MEDICAL TREATMENT

Everyone has the right to refuse to undergo any medical treatment.

Privacy Commissioner's case notes

Each year the Privacy Commissioner receives a number of complaints alleging a breach of the code. From time to time summaries are released about cases which may be of general interest or illustrate a particular point. A case note is not a "precedent" in the legal sense of binding the Commissioner or anyone else. However, it does indicate the approach taken by the Commissioner in a particular case as a guide to how similar cases might be viewed.

Periodically case notes are compiled into indexed volumes, available for purchase. They are also available individually, free of charge, on the Office of the Privacy Commissioner's website at www.privacy.org.nz/case-notes. Contact enquiries@privacy.org.nz if you would like to receive case notes by email when they are issued.

Space is provided below to note the references to other case notes that may be released from time to time.

HEALTH INFORMATION PRIVACY CODE CASE NOTES (AS AT JUNE 2008)

Rule 1: 25766

Rule 2: 5878, 7454, 9482, 15488, 67571

Rule 3: 23887

Rule 4: 9482

Rule 5: 3894, 6656, 21451, 26781, 99263

Rule 6: 0191, 0769, 1666, 3984, 5715, 6656, 7454, 9392, 22968, 26781, 93953

Rule 7: 15376

Rule 8: 14290, 17749

Rule 9:

Rule 10: 5878

Rule 11: 1553, 2049, 5733, 6656, 8649, 9603, 15488, 19461, 21110, 21451, 23067, 23887, 25711, 28873, 30372, 41813, 55528, 67571, 69555, 95042

Rule 12:

Other clauses: 2049, 9603, 17749, 19461, 21110, 41813

Guidance may also be obtained from case notes relating to general complaints made under the information privacy principles (not listed here), which are also available on the Office of the Privacy Commissioner's website at www.privacy.org.nz.

Notes

Notes

Problem with privacy?

If you believe that your privacy may have been infringed and you are looking for guidance, or if you are a health or disability services provider and want information, you can phone the Privacy Commissioner's enquiries line.

In Auckland phone: **09 302 8655**

Other areas phone: **0800 803 909**

Alternatively, email **enquiries@privacy.org.nz**, or visit the Office of the Privacy Commissioner's website **www.privacy.org.nz**

Complaints about privacy?

If you wish to complain about a breach of your privacy, you can:

- check the Office of the Privacy Commissioner's website www.privacy.org.nz under "Your Privacy – How To Complain"
- phone the enquiries line for advice:
  - In Auckland phone: 09 302 8655
  - Other areas phone: 0800 803 909
- or write to:

  The Privacy Commissioner
  PO Box 10094
  Wellington

Health Information Privacy Code 1994

ISBN 0-478-11724-8 (revised edition, 2008)

Further copies are available from the Office of the Privacy Commissioner:

AUCKLAND OFFICE

PO Box 466, Auckland 1140

Level 13, WHK Gosling Chapman,
51–53 Shortland Street, Auckland 1010

Telephone 09 302 8680

Facsimile 09 302 2305

WELLINGTON OFFICE

PO Box 10094, The Terrace, Wellington 6143

Level 4, gen-i Tower,
109–111 Featherston Street, Wellington 6011

Telephone 04 474 7590

Facsimile 04 474 7595

ENQUIRIES LINE

Auckland: 09 302 8655

Outside Auckland: 0800 803 909

Email: enquiries@privacy.org.nz

WEBSITE

www.privacy.org.nz

$25.00 (incl GST)

Design: Beetroot Communications
www.beetroot.co.nz

Printed by: KB Print Ltd
Auckland