PRIVACY AND ACCESS TO INFORMATION

Selene Mize, John Dawson and Nicola Peart

- Common information relationships
- Protecting privacy when collecting, storing and using personal information
- Access to and disclosure of information by others

INTRODUCTION

This chapter provides an overview of New Zealand law concerning privacy and access to information in research. Questions of access to and control over information are clearly vital to researchers. The relevant law is extensive and complicated because questions about information arise in many different forms. Researchers often want access to information held by others, but others may also want access to information held by the researchers. So freedom of information principles go both ways. There are also several different kinds of information, to which different legal principles apply.

This chapter provides no more than a broad outline of the main features of the law. We focus on the issues researchers most commonly confront, particularly matters of privacy when personal material is collected from research subjects and researchers’ attempts to obtain material held by others. Matters arising more occasionally, such as demands from the courts for immediate production of research data, receive only brief mention. In those cases, specialised legal advice is recommended.

We start by suggesting a method through which researchers may analyse information problems. This involves careful scrutiny of the relationships involved: what might be called the information relationships. In these relationships, information in the possession of one party will usually be sought by another. Many of the legal questions then concern how any conflicts between those parties should be resolved. What is the position, for instance, if the party in possession considers it has a duty to maintain the privacy or confidentiality of the information, while the other party considers it has a right of access? We will discuss the standards and procedures the law provides when disputes of this kind have to be resolved.

These disputes are often complicated by the fact that the law may appear to support the opposing contentions of both parties at once. It may appear, for instance,  

---

We gratefully acknowledge the valuable comments of our colleague Associate Professor Paul Roth, Faculty of Law, University of Otago on an earlier draft.
to impose a duty on those in possession to maintain the privacy of sensitive material, while also appearing to confer a right of access to that material on some other person. Obviously, both those contentions cannot stand. To address these situations, the law sets rules about which position takes priority, or procedures for deciding which prevails.

A further complication is the fact that the law does not provide a universal scheme of information protection for all situations. Instead, it provides different rules for different situations, depending on various features of the case. So health information is not covered by the same rules as information about national defence; different rules may apply to information held within the public and the private sectors; and when the police or the Inland Revenue Department demand information from researchers the situation may be different again. As a consequence, it is often necessary to begin the search for relevant principles by examining carefully the position of the parties, the nature of their relationship and the purposes for which the information was initially obtained. When the information concerns an individual, that person's consent to access and use by others will often be critical. When access is sought to published information, on the other hand, or material that is otherwise in the public domain, or anonymised data, few problems will arise.

One common tactic the law adopts when conflicts about information arise is to confer a discretion on the person in possession as to whether to disclose the material. In that situation, the person is given a choice between keeping the material confidential and releasing it to others; the law will not generally interfere with their decision, provided they have approached the matter in the right way. That person may not have an unlimited choice. They may have to exercise their discretion on a specified right basis, taking into account certain matters and then weighing the arguments for and against disclosure in that case. But provided they have properly considered the matter and reached a reasonable conclusion, their decision will stand.

This is a very common legal approach. It frequently applies when outsiders have good reasons to request access to sensitive information. Its effect is to leave the decision concerning disclosure to the person or organisation controlling that information, within parameters specified by law. Provided they operate within those parameters, those responsible may take into account other relevant matters, such as the ethical principles of their discipline or profession.

There are four general positions the law can take on information disclosure:

- it can prohibit it – for example, to protect personal privacy or national security;
- it can require it, thereby providing access to others;
- it can leave the matter to be resolved through an exercise of discretion by a specified person, while indicating the general principles that should be applied;
- it can leave the matter entirely in the hands of the person controlling the information – for example, with private persons who have a free choice whether they will talk to researchers or not.
Common Information Relationships

To organise this discussion, we have divided the relevant information flows – or information relationships – into three kinds.

The first kind of relationship operates between a researcher and an identifiable (and usually living) person about whom sensitive material is collected for the purposes of study (in effect, a research subject). The principal issues here concern the manner of collection, protection by the researcher of the other person’s privacy, the proper use and storage of sensitive data, and the scope of the exceptional situations in which such material might be passed by the researcher to a third party without the subject’s consent. There is also the question of the subject’s right to obtain later access to the material collected about her or him, and to exercise control over its use. These are largely matters of privacy law.

The second set of relationships arises when a researcher seeks access to information, and that information is either not private material about a specific individual at all, or it is held by some other person or agency, not the person concerned (that is, it is held by
a government department or company or hospital, perhaps, or some other citizen or group). Similar issues can arise here as in the researcher-subject relationship, concerning the need to protect personal privacy against unauthorised disclosure, and there is considerable overlap in the principles that apply. But this is a distinguishable situation from that in which information is flowing directly between researcher and subject, and some different principles apply.

With regard to this second set of relationships, the law makes an important distinction between the position of public sector agencies that are subject to the Official Information Act 1982 and the Local Government Official Information and Meetings Act 1987, and those persons or agencies that are not subject to the official information act regime (which includes all private businesses, organisations and individuals, unless they happen to be acting on behalf of a public sector agency at the time). Public sector agencies are subject to the general principle of the official information regime – known as the ‘principle of availability’ – which requires them to produce information they hold on request, unless there is a ‘good reason’, stated in the Act, for it to be withheld. Private sector agencies and private persons, on the other hand, are not subject to the same principle, and, as a result, they can often choose whether to disclose material to researchers or not. They may do so, provided they do not breach any other rule of law but, unlike most public sector agencies, they are not under a prima facie obligation to help researchers at all.

The third set of relationships concerns the situation that arises when outside parties, beyond the researcher-subject relationship – such as the police, media, other researchers or commercial enterprises – seek access to a researcher’s data or results, or, having obtained it, they seek to use it in a manner to which the researcher is opposed. What legal tools are then available to the researcher to protect research data from such access or use by others? Will the law ever force an unwilling researcher to disclose material to ‘third parties’ in such a case?

A special variant of this situation occurs on the rare occasions when courts demand the production of material collected by researchers. They may demand material that relates to the commission of a crime, for instance, or material that may be relevant as evidence in some other legal proceedings. Tribunals and commissions of inquiry may also make such demands. What is the researcher’s position then?

It is around these sets of relationships that this chapter is structured. We would encourage researchers to start their analysis of privacy and information problems by characterising the relationships in this way.

A Short Summary of the Relevant Law
The main legal principles in this field can be summarised as follows:

- Duties of non-disclosure are often imposed on those who collect or hold sensitive information, especially private material about individuals and material received in confidence, which should not usually be disclosed without the consent of the person concerned. The Privacy Act 1993, the Health Information Privacy Code (in the
case of 'health information') and the law regarding confidentiality are the principal sources of rules.

Nevertheless, there are many recognised exceptions within these rules under which disclosure of such information without the subject's consent is either permitted or required. These disclosures promote other important interests, to which the law gives higher priority on some occasions, such as the need to prevent serious harm, promote health, and promote research in the wider public interest.

- All individuals have a prima facie right of access to information about themselves that is held by organisations, businesses, professionals and researchers, including a right to control in some respects how that information is collected and used. This is a further aspect of the privacy regime.

- In addition, New Zealand citizens and others present in New Zealand have a prima facie right of access to 'official information' held by public sector agencies covered by the Official Information Act (this includes universities, CRIs, public health authorities and public funding agencies). The Official Information Act still provides 'good reasons' for such information to be withheld, however, including the need to protect personal privacy when that is more important than the interests advanced by disclosure.

- There is a further body of law concerning complaints, remedies and penalties when privacy is breached, or confidentiality broken, unlawfully. The Privacy Commissioner, the Ombudsmen, the courts and professional disciplinary tribunals may all be involved in considering these complaints.

- The police may be authorised by law to obtain search warrants, or subpoenas, for the compelled production of evidence of criminal offending; and some other public sector agencies, such as the tax department, are authorised to gather information under statutory powers. Clear legal powers of this kind, to demand production of information, prevail over privacy rights on most occasions.

- The courts may also order the production of otherwise private or confidential material for use by parties in legal proceedings. Those who wish to resist such claims may try to rely on the law of privilege, which excludes certain material from disclosure or bans its admission as evidence in court.

In the rest of this chapter we explain these principles at greater length and indicate how they apply to research.

**Protecting Privacy when Collecting, Storing and Using Personal Information**

Researchers often gather highly personal and sensitive information, particularly from human research subjects. Important privacy principles then apply. The major provisions affecting the collection and storage of such information are in the Privacy Act 1993. We summarise these below. Before doing that, we need to distinguish two related concepts which are easily confused, those of privacy and confidentiality.
Proper adherence to this principle will require careful advance planning, but researchers will not be liable for all security failures; they are only required to take reasonable steps to protect data. It has been recognised by the Commissioner that occasional human error can be difficult to prevent, and that misconduct by ‘rogue’ employees does not mean reasonable security safeguards were not in place. Any assessment of a security system will look at its cost and workability, the risks involved, the sensitivity of the information, and other safeguards in place.

IPP 6: INDIVIDUALS MUST BE GRANTED ACCESS TO THEIR PERSONAL INFORMATION

When individuals request access to information about themselves, the Privacy Act or a code of practice applies, not the Official Information Act. If a proper request is made, the individual must be told whether information is held about him or her and granted access to it unless an exception applies. There are no significant differences here between the IPPs and the Rules of the HIPC. There are many grounds upon which such requests can be refused (provided by ss 27 to 32 of the Privacy Act), but few that are likely to apply in the context of research.

The relevant grounds for refusing an individual access to his or her personal information are:

- danger to the safety of any individual (s 27(1)(d)) – for example, another person has supplied unfavourable information about a subject who might make a punitive response;
- prejudice to any person’s physical or mental health (s 29(1)(c)) – for example, risk of suicide or emotional problems if research results are disclosed;
- unwarranted disclosure of another person’s affairs (s 29(1)(a)) – for example, private information provided by other members of a research subject’s family;
- refusal necessary to protect trade secrets or prevent commercial damage to the supplier or subject of the information, unless this is outweighed by the public interest in its disclosure (s 28(1)) – for example, a research subject wants to know the exact details of an experimental drug administered, or to know why she or he was rejected for a drug trial;
- it is evaluative material, such as information provided by referees, or gives the referees’ identity, and was given in confidence (s 29(1)(b));
- the information is not readily retrievable (s 29(2)(a));
- the information does not exist or cannot be found (s 29(2)(b)).

Other exceptions include situations where disclosure would prejudice the maintenance of the law or damage the interests of a young person, and certain

---

10 Roth at C 91C, quoting Case No 26280 of the Privacy Commissioner’s Case Notes.
11 Roth at C91H4, quoting the Assistant Privacy Commissioner.
12 The Official Information Act, Part IV, applies to access requests made by corporations (which are considered ‘legal persons’).
information held by libraries, archives or the police. Note that interference with a research project is not a reason for denying access. If subjects in a double-blind clinical trial demand to know whether they have been given the experimental drug or a placebo, they must be told, even if this means they must be withdrawn from the trial. Only material covered by an exception may be withheld; access must be given to other information, even in the same file. The material held back can be deleted or removed from the file supplied, or access can proceed under supervision.

Access is subject to certain procedural requirements (ss 33 to 45). On receiving a request, the researcher must ascertain the identity or authority of the requester and release information directly to him or her (for example, using registered mail). Assistance must be given and referrals made as required. Decisions on requests must occur within twenty working days, and sooner if practicable. The requester must then be told whether the request will be granted and how any information will be released. If access is denied, reasons must be given (s 44). Individuals may complain about denial of access to the Commissioner. If the information is held by a public sector agency, access requests are also enforceable in court (s 11). Whenever individuals make requests for access to their personal information, they must be advised that they may request its correction.

If the requests for access concern health information made by individuals or their representatives, this must be considered under HIPC Rule 6, but an agency may refuse to disclose such material to the representative if it would be contrary to the individual's interests; or the agency has reasonable grounds for believing the individual would not support disclosure of that kind; or one of the usual exceptions applies.

IPP 7: INDIVIDUALS MAY REQUEST CORRECTION OF THEIR PERSONAL INFORMATION

Both IPP 7 and HIPC Rule 7 provide that the subject of personal information is entitled to request its correction. The agency is not obliged to change the information in the way requested; it need only take reasonable steps to ensure it is accurate, up to date, complete and not misleading. The agency must inform the individual of the action taken. If no change is made, the agency must take reasonable steps to attach a statement to that effect to the material if that is what the individual requests. If the agency takes

13 Paul et al. at 206–207.
14 HIPC at 31.
15 HIPC at 32.
16 Ibid.
17 Privacy Act 1993 s 6; IPP 6(2); HIPC Rule 6(2).
18 These exceptions apply also to requests for access to information under s 22F of the Health Act 1956: N. Peart, 'Access to, and Disclosure of, Health Information: Are the Rules in Need of a “New Treatment”?' (1996) 2 Human Rights Law and Practice 95.
19 Section 55 of the Act lists exceptions to this principle, including evidence given to a commission of inquiry and correspondence with the Ombudsman or Commissioner.
steps to correct the information or attaches a statement, it must then take reasonable steps to inform people to whom the information has been disclosed.

IPP 8: Accuracy of Information must be Checked Before Use
IPP 8 and HIPC Rule 8 require agencies to take reasonable steps to ensure personal information they hold is accurate, up to date, complete, relevant and not misleading, having regard to its purpose. Verifying information will be especially important if collected from a source other than the individual or it is important or sensitive. Some researchers show drafts of such material to subjects prior to publication. The reason is mostly to protect personal privacy, but this practice also helps ensure accuracy before use and permits corrections to be made.

IPP 9: Information must not be Kept Longer than Necessary
This rule forbids keeping personal information longer than required for any purpose (not necessarily the original purpose) for which it may lawfully be used. The Commissioner has indicated that researchers wishing to keep identifying information longer than required for the original project should obtain ethics committee approval.20 But some legislation requires researchers to keep data for a specified time.21 IPP 9 adds that agencies can still keep any health information for the purposes of providing health or disability services to that individual.

IPP 10: Limits on Information Use
This rule concerns the use of personal information for purposes other than those for which it was originally collected. If a researcher has fully specified these purposes when obtaining it, this principle will not apply. IPP 10 will usually prevent use of information for new purposes that the individual has not authorised unless there is a reasonable belief that:

• the information is publicly available;
• use of the information is necessary to lessen a serious and imminent threat to health or safety of the public or an individual;
• the new purpose is directly related to an original purpose;
• the information will be used in an anonymous form.

HIPC Rule 10 is similar. In addition, it permits new uses of health information when authorised by the individual's representative, if the individual is incapacitated. It requires ethics committee approval to be obtained to make new anonymous use of such material in research.

20 HIPC at 40.
21 For example, Health (Retention of Health Information) Regulations 1996; Hospital Regulations 1993, cl 8; Medications Regulations 1984, cl 58.
Access to and Disclosure of Information by Others

We now turn our attention to contested questions about access to information and its disclosure. These issues are obviously vital to many researchers, but they are complicated because they can arise in many different forms. As explained earlier, access to and disclosure of information may be two sides of the same coin, or two aspects of a single relationship. One party will be seeking access to information which another party may disclose. To the former, the matter may seem to implicate a right of access, to the latter it may seem to be a question of lawful disclosure.

Researchers can find themselves on either side of this relationship. They often seek information from others to advance their work, but others may also seek information from them. Researchers should bear this in mind when advocating liberal policies on access to information. Those policies might later be applied to their research, even before it is published.

The essential legal matters concern the respective spheres of operation of the Official Information Act and Privacy Act regimes and their rules concerning access and disclosure. To understand the area fully, several important distinctions have to be grasped between:

- disclosures that are prohibited, permitted and required;
- disclosure of material governed by the Official Information Act and not governed by the Official Information Act;
- disclosure of personal information as opposed to other kinds of information.

Disclosures that are Prohibited and Permitted and Required

Some disclosures are contrary to the law – meaning some form of penalty, such as damages, or another sanction, could apply. They are prohibited. A health authority disclosing personal health information to a researcher without the patient’s consent, when no recognised exception to privacy principles applies, is a case in point.

The distinction between permitted and required disclosures is more subtle. When disclosure is permitted, the person in possession of the information has a discretion to release it or not. If the discretion is properly exercised, it would be lawful to do so, but not mandatory. The corollary is that the person who makes the request for such information has no right to the information, but is simply entitled to make a request. The person in possession has the ultimate power to decide. All the disclosure rules provided by IPP 11, HIPC Rule 11, and s 22C of the Health Act – discussed below – are of this kind. They permit disclosure of personal information in some cases, but do not require it. This is very important for researchers to understand. It means they may not get the material they want even if a privacy exception applies. The final decision is within the discretion of the data-holder. In most cases, data holders are not even required to tell researchers what information they do hold.
There are situations in which disclosure is required by law. In that case, the person or agency making the request has a genuine right of access that could be enforced in court or through some other mandatory process. The Official Information Act regime is of this kind. The essence of its 'principle of availability' is that when there is no 'good reason' to withhold the requested material, disclosure is required. It is genuine 'freedom of information' legislation. Not every right of access it provides is immediately enforceable in a court. A prior complaint to the Ombudsman or Privacy Commissioner may be required. But if disclosure is improperly resisted, it still can be ordered.

Disclosure is also mandatory when courts order the production of material, either to them, or to others at their direction, as with disclosure to the police or the Child, Youth and Family Service for the purpose of legal proceedings. On rare occasions, a 'privilege' can be invoked to resist such disclosure, and some researchers who have received material in confidence from subjects may convince the court to exercise its discretion to excuse them from giving evidence in court about that material. But if the court insists on disclosure, the mandatory element is very clear. Refusal to disclose upon a court order is contempt of court, punishable by a fine or imprisonment. Researchers should keep this in mind whenever tempted to offer 'absolute' confidentiality to research subjects.

The Priority of Specific Legislation

There are many provisions, scattered through the statute book, under which disclosure of certain kinds of information is specifically prohibited, permitted or required. Many of these mandatory disclosure provisions relate to health, safety, social welfare or taxation. A very important legal principle is that, in a case of conflict, these specific provisions will prevail over the general rules provided by the privacy and official information regimes. They therefore should be obeyed.

Mandatory disclosure provisions are especially relevant to health and disability researchers whose research also involves clinical care. In their research, these clinician-researchers may discover things about a person's health that they may later be required to disclose. Examples are:

- disclosure of health records on the request of other health professionals treating the same person, or at the request of the person's representative, unless reasonable grounds exist to believe the patient does not approve, or that would be against the patient's interests (s 22F Health Act; Rule 11(4) of the Health Information Privacy Code);
- disclosure to the Health and Disability Commissioner investigating a complaint (s 62 Health and Disability Commissioner Act 1994);

---

Disclosure to the registration bodies of some health professions concerning disabled professionals continuing in practice and placing others at risk, as required by the statutes regulating various health practitioners.

There are also many specific provisions that permit clinician-researchers to disclose health information to third parties without the patient’s consent. They may disclose, for example:

- to the persons, and for the purposes, listed in s 22C of the Health Act – for example, disclosure to statutory officials (including social welfare authorities, community corrections, prison doctors, Ministry of Health, the army) to perform their statutory functions;
- to report suspected child abuse (ss 15, 16 Children Young Persons and their Families Act 1989);
- in a form that does not enable identification of the subject (s 22H of the Health Act).

Requests for Information Covered by the Official Information and Privacy Regimes

So far we have been talking about three main kinds of information: official, personal and health information. Each is covered in some respects by a separate legal regime. We now try to indicate more clearly the circumstances in which these different regimes apply, particularly the respective spheres of operation of the official information and privacy regimes.23

The general relationship between these different kinds of material is indicated in this diagram:

![Diagram showing the relationship between official, personal, and health information]

**Figure 5.2: Relations between three main forms of information**

---

There is overlap in how these categories are defined. 'Personal information' is defined simply in s 2 of the Privacy Act as 'information about an identifiable individual'. 'Health information' is defined in clause 3 of the HIPC. Generally speaking, it is information about an identifiable individual that pertains to her or his health (or disabilities) or the delivery to the person of services in those areas. It is therefore a special subcategory of 'personal information'. It is covered expressly by the HIPC.

'Official information', on the other hand, is defined in s 2 of the Official Information Act as information that is held by a wide range of specified public sector organisations, subject to a few exclusions, such as material held by the courts, to which special regimes apply.24

Some of this official information is about identifiable individuals, such as the records held by the social welfare and tax authorities and the police. We call this 'personal official information'. Large amounts of 'health information' are also held within the public sector – notably within the public health and disability services, but also in large public health registers and databases maintained by the Ministry of Health. This material is a special sub-category of personal official information. On the other hand, the records held by private health professionals, such as most GPs, are not of this kind. They contain personal health information, which is covered by the HIPC under the Privacy Act regime, but they are not covered by the Official Information Act. The diagram above clearly indicates the position overall.

The key legal question is: which legal regime applies to requests for personal official information when the categories overlap? One might think the Privacy Act regime would apply, because personal information is its main concern, and that regime applies when individuals make requests for personal official information about themselves. But when the request for personal official information is made by someone else, the current weight of legal opinion is that the official information regime applies to its disclosure – even if it is health information – although the matter has not been finally determined by a court.25

This does not mean the Privacy Act regime is irrelevant in such cases. Protecting personal privacy is a 'good reason' for refusing to release information under the Official Information Act, if there are no competing public interests having more weight. The privacy regime is an authoritative source of guidance on what privacy demands. Its principles should therefore be closely considered by those acting

---

25 This is the position taken by the Ombudsmen in their Practice Guidelines No 6, 1994; and by the authors of standard texts on New Zealand privacy law: see Roth at C/97–98, and E. Longworth and T. McBride, The Privacy Act: A Guide (Wellington: GP Publications, 1994).
under the official information regime: they have to weigh the privacy concerns against the other interests, to decide whether there is a good reason for personal information – held within the public sector – to be withheld from third parties.

**INFORMATION Governed by the Official Information Act**

The Official Information Act governs access to information held by public sector agencies. Researchers may request access to such information, or they may be subject to an official information request, if they work within (or act as an agent of) a public sector agency to which the Act applies.

**Official information defined**

The Act applies to 'official information'. This is defined in section 2 as information held by:

- a government department listed in the First Schedule to the Ombudsmen Act;
- a Minister in his or her official capacity;
- an organisation listed in the First Schedules to either the Official Information or the Ombudsmen Acts.

In addition to government departments, the number of organisations covered by the Act is extensive and includes such agencies as Crown Research Institutes, the Health Research Council, universities (and their academic staff), ERMA, ACC, district health boards, Meridian Energy, Industry New Zealand, FRST, the New Zealand Antarctic Institute, the National Animal Ethics Advisory Committee, and so on.

Information held by an officer, employee or member of a department or organisation subject to the Act is deemed to be held by that department or organisation. Through this provision, the regional ethics committees and the National Ethics Committee on Assisted Human Reproduction may come under the Act’s regime. These committees are administered and resourced by the Ministry of Health and their administrators, who hold their records, are employees of the Ministry.

Organisations not listed in the schedules are not subject to the official information regime. The courts, tribunals (in relation to their judicial function), Royal Commissions and commissions of inquiry are explicitly excluded.

**Requests for official information**

The process for requesting access to official information is laid down in sections 12 to 19. New Zealanders and anyone in New Zealand may make a request to a public sector agency. The information must be specified with due particularity. The agency receiving the request is obliged to give reasonable assistance.

---

26 Very similar legal principles are applied to local government by the Local Government Official Information and Meetings Act 1987.
The agency must, within twenty working days of receiving the request, notify the requester whether it will be granted, and, if so, the manner of access and the charge. The agency may extend the time limit if a lot of material is requested, or is to be searched, or the necessary consultations require extra time.

If the agency does not hold the information, but believes it knows who does, the request must be passed to the other agency within ten working days. That party must also pass on the request if it believes it is more closely connected with the functions of another department or organisation. The agency to whom the request has been transferred then has twenty days to respond.

The principle of availability and its major exceptions

The fundamental principle of the official information regime is that information held by the public sector agencies covered by the Act should be made available to anyone who requests it, unless one of the exceptions in the Act or some other statute applies (s 5).

The exceptions to this principle fall into three categories. The first category provides for withholding official information (s 6). It may be withheld if its disclosure is likely to:

- prejudice the maintenance of the law;
- prejudice the security or defence of New Zealand or its international relations;
- endanger the safety of any person;
- seriously endanger the economy of New Zealand.

The second category of exceptions to the principle of availability requires a balancing of conflicting interests. Section 9 lists a number of other 'good reasons' for withholding official information, but unlike the reasons in the first category, these reasons may be outweighed by other considerations that render it desirable in the public interest to make the information available.

These reasons for withholding information under s 9, to be balanced against the arguments in favour of disclosure, include:

- protecting the privacy of living or dead people;
- protecting trade secrets;
- unreasonable commercial prejudice;
- protecting information provided in confidence;
- maintaining constitutional conventions concerning the confidentiality of Cabinet, and of its relations with the Crown, and of communications between Ministers and public servants;
- protecting the confidentiality of legal advice prepared in contemplation of litigation;
- prejudicing the supply of similar information, or information from the same source;
- prejudice to measures protecting health and safety of members of the public;
prejudice to substantial economic interests of New Zealand;
• preventing prejudice to negotiations;
• preventing its use for improper gain or advantage;
• preventing improper pressure on public servants;
• some other disclosures likely to damage the public interest.

Any of these reasons may justify withholding information requested or held by a researcher, but in each case the person holding the information will have to consider whether there is an overriding public interest in making the information available. For example, a researcher may request access to information held by a government department about the living arrangements of members of Parliament. While such information might be withheld on privacy grounds, the interests of public accountability may outweigh the privacy concerns, thus imposing a duty on the department to make the information available.

Alternatively, it may be the researcher to whom the request for information is made. For example, some university scientists may have made a discovery that is subject to a patent application lodged by them. If they were asked to make their results available prematurely, their patent application might be jeopardised. They could argue that disclosure of their findings would unreasonably prejudice their commercial position. They would also be entitled to withhold the information if the person requesting it was trying to gain an improper advantage, such as using it to further their own research or publication record. In any of these situations, it is unlikely that there would be an overriding public interest in making the information available.

The third category of exceptions is listed in s 18. This permits a request for official information to be refused on the following additional grounds:
• the agency can neither confirm nor deny its existence, because that would prejudice the interests protected conclusively by s 6 (see above), would disclose a trade secret or would impose unreasonable commercial prejudice;
• the disclosure would be in breach of a statute or constitute contempt of court;
• the information is or will soon be publicly available;
• the document said to contain it does not exist or cannot be found;
• it cannot be made available without substantial collation or research;
• it is not held and there is no reason to believe it is held by another relevant agency;
• the request is frivolous or vexatious or the information requested is trivial.

It is important to note that the Official Information Act authorises the withholding of information if one of the ‘good reasons’ applies, but does not require it to be withheld. If a request for official information is refused, the agency must give the applicants the reason and, if the applicants request, the grounds to support that reason. Reasons need not be given, however, if that would prejudice the interests protected by ss 6 or 9 and, in the case of s 9, there is no countervailing public
interest. The applicants must also be informed of their right to make a complaint to the Ombudsman seeking an investigation and review of the refusal. This review may result in a binding recommendation being made against the agency.

Withholding 'Personal Official Information' to Protect Privacy

When a request is made by a third party for access to 'personal official information' the position is covered by these principles under the Official Information Act. This includes requests by third parties for information in the medical records of public hospitals, and all personal information held by researchers in the public sector.

As explained, the general policy of the Act is to make official information available unless there are good reasons not to (ss 4(c) and 5). One good reason is protecting personal privacy (s 9(2)(a)). But it is not sufficient to identify the privacy concerns. The information holder must go further, in the balancing of interests under s 9, to consider whether 'in the circumstances of the particular case' the privacy interests that support 'the withholding of the information [are] outweighed by other considerations which render it desirable in the public interest, to make that information available'.

There are therefore two steps in this decision. The privacy concerns must be identified, then they must be weighed against any other public interests that would nevertheless favour disclosure of the personal information to a third party. Only if the privacy concerns predominate may the information be withheld.

A wide range of factors may be relevant to this calculation. The extent of the intrusion on personal privacy should be carefully considered, with the general principles of the Privacy Act regime (including the Health Information Privacy Code) as important indicators of what privacy requires. The person to whom the information relates should also be consulted, if practical. But the views of those whose privacy is threatened are not conclusive, because the competing public interests that favour disclosure must still be given full weight. On occasions, the strong public interest in facilitating certain kinds of research (for example, with important implications for public health or safety, or enforcement of the law) may still prevail over privacy concerns, leading to disclosure.

A very important aspect of the official information regime is that it requires such disclosure when no good reasons to withhold apply. There may be an element of discretion in the balancing of competing interests by those who control official information, but once they decide the balance favours disclosure, the material must be disclosed. It would still be good practice, if practical, to inform those whose privacy is threatened that disclosure will occur, to comply with the spirit of the privacy regime.

Disclosure of Personal Information under the Privacy Regime

Where personal information is not also official information, requests for it are handled under the Privacy Act regime, in particular, IPP 11 or HIPC Rule 11.

Such disclosures to third parties, in circumstances authorised by the Privacy
regime, are always discretionary, however, not mandatory. The information holders may take many factors into account, including ethical principles. In particular, they must take into account any other principle of law that counts against disclosure in that case: for example, based on any agreement or undertaking not to disclose the material, or its confidential character. If other legal principles of this kind forbid disclosure, they prevail.

If no other legal principle forbids disclosure, careful consideration should be given to the exceptions to disclosure found in IPP 11, or HIPC Rule 11 (in the case of health information).

**IPP 11: Limits on disclosure of personal information**
Under this principle, disclosure of personal information for a new purpose without the consent of the subjects or their representatives may still be lawful:

- when the information will be used in anonymous form;
- to prevent or lessen a serious and imminent threat to public health and safety or that of an individual;
- when the information ‘is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned’ (IPP 11(h)(ii)).

Under this last exception, personal information can be passed lawfully to researchers in identifying form, if no other prohibition applies, provided the material is anonymised in subsequent publications. It would be reasonable for data-holders to require a written undertaking to that effect from the researchers.

These disclosure principles should also guide those weighing the interests for and against the release of private material under the Official Information Act.

**Rule 11 of the Health Information Privacy Code**
If personal health information is involved, the exceptions permitting non-consensual disclosure are narrower. In particular, the exception for research applies only when three criteria are met:

- those holding the information ‘believe on reasonable grounds that it is either not desirable or not practicable to obtain authorisation [to disclose] from the individual concerned’ (Rule 11(2));
- the information is ‘to be used for research purposes (for which approval by an ethics committee, if required, has been given)’ (Rule 11(2)(c)(iii));
- the information ‘will not be published in a form which could reasonably be expected to identify the individual concerned’ (Rule 11(2)(c)(iii)).

The critical difference in these Rules is the reference to approval by an ethics committee. It is not entirely clear in New Zealand when ethics committee approval is ‘required’, especially if this means ‘required by law’ (see chapter 3 on research ethics committees). But disclosure of health information under this research exception is...
discretionary, in any case, and any careful medical record-holder will insist on ethical approval being obtained, as a matter of professional ethics. So approval by an ethics committee will almost certainly be required in practice when such material is passed to researchers in identifying form. When applying for ethical approval, researchers should state why it is not practicable or desirable to obtain consent from the person or his or her representative. The material must then be anonymised by the researchers for publication.

**Disclosure of Other Material Held in the Private Sector**

With regard to other kinds of information – not personal or official information – that is held in the private sector, and is not covered by either the Official Information Act or the Privacy regimes: its disclosure to researchers is largely a matter of choice for the persons or organisations concerned. There are some laws requiring private sector disclosures to facilitate research. The Cancer Registry Act 1993, for instance, requires private pathology laboratories to send all positive cancer test results to the national cancer registry, to advance cancer research. But these examples are rare. There are also the legal rules that prohibit disclosure of some material, even by private organisations or individuals, when that would breach a rule of law, such as the rules concerning confidentiality. But if there is no legal prohibition on disclosure, the matter is entirely within the discretion of private organisations. It is to be hoped that they will assist worthwhile research, but that is not an obligation imposed by law.