Protecting health information privacy in research: how much law do Australians need?

Colin J H Thomson

ABSTRACT

- Privacy regulation in Australia, whether by federal or state legislation or other means, has provoked complaints from researchers.
- Its scope depends on defining the information it covers, the organisations it governs and the principles it applies.
- Regulation is inconsistent, and compliance can be complex (as illustrated by a hypothetical research example).
- National reform to achieve a realistic, balanced, publicly acceptable and consistent regulation is urgently needed, and has been recognised and recommended by recent reviews of the *Commonwealth Privacy Act 1988* (Cwlth) by the Office of the Federal Privacy Commissioner and the Australian Senate.

MJA 2005; 183: 315–317

The extension of the *Commonwealth Privacy Act 1988* (Cwlth) to the private sector and, in particular, to the collection, use and disclosure of health information, has provoked complaints about the negative effects on health practice and research. Furthermore, the Australian Capital Territory,[1] the Northern Territory,[2] New South Wales[3] and Victoria[4] have enacted legislation protecting privacy in health information. Other state governments rely on administrative practices in the exercise of their responsibilities for health information held in state hospitals or departments. In research that depends on access to collected health information, it is necessary to sort out how to comply with multiple legislative requirements. This article examines the difficulties that researchers face in this task.

Interpreting privacy statutes

Privacy legislation and many of the guidelines are complex examples of structure and language, but the key definitional issues are:

- What information is caught by the legislation?; and
- What organisations are caught by the legislation?

What information is caught by the legislation?

The central concepts are "personal information", "sensitive information" and "health information" and, to understand the last of these, "health service". In the Commonwealth Privacy Act (and almost all other legislation),

> "personal information" means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.[5]

This definition has a quality of "intrinsic identifiability", meaning that what can be used to identify a person must be contained *in the information itself*. It follows from this that, if information lacks such elements, handling of it is not governed by the Privacy Act. So, information that contains details of a health condition of a person, identified by a code number, is not personal information if there is nothing in the information itself by which the identity of that person can be reasonably ascertained.

Sensitive information is a subset of personal information, and is information about matters like racial or ethnic origin, political opinions, membership of certain organisations, and health. It is important to know what falls into this definition, as tighter limits are imposed on handling sensitive (and therefore health) information.

National Health and Medical Research Council, Canberra, ACT.
Colin J H Thomson, BA, LLB, LLM, Consultant in Health Ethics.
Reprints: Professor Colin J H Thomson, National Health and Medical Research Council, GPO Box 9848, MDP 24, Canberra, ACT 2601.
Colin.Thomson@nhmrc.gov.au

In the Commonwealth Privacy Act, *health information* and *health service* have specific definitions, as shown in Box 1.

The combination of these definitions means that all (identifiable — remember that health information is personal information) information about a person's health, or information that is collected in the course of treating or used to treat that person, is governed by the Commonwealth Privacy Act. Definitions of these expressions in state legislation are not identical.

1 Definitions of "health information" and "health service" under the *Commonwealth Privacy Act 1988* (Cwlth)

Health information

(a) information or an opinion about:

(i) the health or a disability (at any time) of an individual; or

(ii) an individual's expressed wishes about the future provision of health services to him or her; or

(iii) a health service provided, or to be provided, to an individual;

that is also personal information; or

(b) other personal information collected to provide, or in providing, a health service; or

(c) other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances.[5]

Health service

(a) an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the person performing it:

(i) to assess, record, maintain or improve the individual's health; or

(ii) to diagnose the individual's illness or disability; or

(iii) to treat the individual's illness or disability or suspected illness or disability; or

(b) the dispensing on prescription of a drug or medicinal preparation by a pharmacist.[5] ◆

What organisations are caught by the legislation?

Whether the person or organisation handling personal information is bound will depend on the definition of one or more of "organisation", "agency" and "authority". The Commonwealth Privacy Act, in its application to the public sector, defines *agencies* as including all Australian government departments, agencies and instrumentalities.

In its application to the private sector, the same Act defines *organisation* as:

> (a) an individual; or
>
> (b) a body corporate; or
>
> (c) a partnership; or
>
> (d) any other unincorporated association; or
>
> (e) a trust;
>
> that is not a small business operator, a registered political party, an agency, a state or territory authority or a prescribed instrumentality of a state or territory.[6]

A small business is one that has an annual turnover of $3 million or less, *but does not include any small business that provides a health service to another individual and holds any health information except in an employee record*. This means that medical professionals and health care institutions are required to conform to the legislation.

State legislation, in its application to state public sectors, uses wide definitions of organisations.[7-9] In relation to the private sector, state legislation in NSW and Victoria applies to organisations that are health service providers. The definitions of these terms are more detailed than that of a health service in the Commonwealth Privacy Act.

Structural features of privacy legislation

Privacy legislation is generally similar in structure. Agencies or organisations (to which the legislation applies), are required to conform to a set of privacy principles when collecting, using and disclosing personal information (to which the legislation applies). The principles are called Information Privacy Principles (when applied to Australian government agencies), National Privacy Principles (when applied by the Commonwealth Act to the private sector) and Health Privacy Principles (in both the NSW and Victorian Acts). No set of principles is the same as any other, although the differences between the two state sets of Health Privacy Principles are least.

Broadly speaking, the structures have similar elements:

- The collection of health information conforms, if conducted fairly, with notice of the intended purpose so that individuals are aware of disclosure practices.
- Use or disclosure of health information is always permitted with consent.
- Use or disclosure without consent is lawful in emergencies, for law enforcement or when authorised by law.
- Non-consensual use and disclosure are also lawful if for defined purposes and subject to defined conditions, including a privacy review by a human research ethics committee.

There are important differences in the prescription of these conditions between and among the sets of principles.

Failure to meet the relevant principles means that an individual's privacy has been infringed without justification. Enforcement of privacy regulation requires a complaint that can trigger an investigation by the relevant (federal or state) officer with a view to resolving the complaint. That resolution can involve the payment of compensation. With the exception of Australian government agencies, only deliberate conduct to avoid or subvert privacy legislation involves a statutory offence.

2 Hypothetical study to identify a genetic marker for early-onset osteoporosis

In one state, two institutions — a state hospital and a private hospital — operate osteoporosis clinics. To identify potential research participants, a researcher proposes to:

- Ask each hospital to review their medical records to identify women under the age of 45 who have been diagnosed with osteoporosis or have had two or more fractures of the hip, ankle or wrist in the past 5 years; and
- Seek access to records of female recipients of a disability support pension held by the Australian Government Department of Social Security who have been similarly diagnosed.

If potential participants can be identified, the researcher will ask the hospitals to disclose the identifying information for these women. The researcher will then contact the women to invite them to participate in the research project which will involve a survey, a bone density test and the testing of a blood sample for a genetic marker which may be an indicator of early-onset osteoporosis.

Women can consent or refuse to participate. ◆

An example of health research

To demonstrate briefly how these variations could complicate a research project, an hypothetical study is outlined in Box 2.

The Australian government agency

The study involves personal information held by an Australian government agency (the Department of Social Security) which is to be used for medical research, but without any consent. The agency can only disclose the information if a human research ethics committee (HREC) reviews the privacy implications, using the guidelines that relate to the Information Privacy Principles (the section 95 guidelines).

The private hospital

Health information is held by the private hospital which provides a health service, so that National Privacy Principle 2.1 in the federal legislation applies. This is because, in reviewing the records, the hospital is *using* the information for research and not for the original purpose for which it was collected, which was treatment. The research purpose is not a directly related secondary purpose of which the individuals would have been made aware when the information was collected. The hospital would need to decide whether it is practicable for it to seek consent from the individual women. If it decides it is not practicable, an HREC, using the guidelines on the National Privacy Principles (guidelines under section 95A), can review the proposal to decide whether the public interest in the research outweighs substantially the public interest in protecting privacy. Even if the HREC does so decide, the hospital may still decide not to permit use or disclosure.

If the hospital is in NSW or Victoria, state legislation also applies. Similar decisions must be made by the hospital and by an HREC. While the decision about impracticability to seek consent is required, state legislation adds additional tests of whether the purpose can be achieved by using non-identifying information,

whether steps can be taken to de-identify the information, and whether the results will be published in a non-identifying form. The federal and state legislative definitions of research are not identical, nor is the description of the link between the information and the research: federal legislation requires the information to be "necessary", while in state legislation, "reasonably necessary" is sufficient.

The state hospital

Health information is held by the state hospital, conducted by a state agency, from which the researcher seeks disclosure. The Commonwealth Privacy Act does not apply because state agencies are excluded from the federal legislative definition of organisation. State regulation applies: whether specific legislation (as in NSW and Victoria) or regulatory instruments (as in Queensland) or administrative directions (as in South Australia and Tasmania), or administrative practices (as in Western Australia).

If the hospital is in Victoria, the *Health Records Act 2001* (Vic)[4] and the *Information Privacy Act 2000* (Vic)[10] permit disclosure if it is reasonably necessary for research in the public interest, it is impracticable to seek consent, the agency believes that the recipient will not disclose the information, publication does not identify individuals, and there is a favourable HREC review.

If the hospital is in Queensland, Information Standard 42A imposes the same criteria as the federal National Privacy Principles. It must be impracticable to seek consent and an HREC must complete a favourable review, using the guidelines under Information Standard 42A. However, section 62F of the *Health Services Act 1991* (Qld)[11] permits disclosure of information without consent only if the chief executive of the state health department considers it in the public interest.

If the hospital is in SA, a Cabinet Instruction, based on federal Information Privacy Principles, governs use and disclosure. That instruction does not permit relaxation of those standards, although the Privacy Committee may exempt the hospital, on conditions, from the requirements.

If the hospital is in WA, the proposal for use and disclosure of the information will be reviewed by the Confidentiality of Health Information Committee.

If the hospital is in NSW, both the *Privacy and Personal Information Protection Act 1998* (NSW)[12] and the *Health Records and Information Privacy Act 2002* (NSW)[3] will apply. Directions under the former Act permitted relaxation of its limits on disclosure. The latter Act permits disclosure if the information is reasonably necessary for research, if either the purpose cannot be achieved with non-identifying information or steps are taken to de-identify the information, results are not published in a form that identifies individuals and there is an HREC review that favourably determines the balance of public interests.

If the research is conducted at a national level and health information is needed from public and private hospitals in all states and territories, all of these differences would apply to the same project.

Conclusion

Health professionals have relied on ethical and legal principles of confidentiality in their collection, use and disclosure of health information, whether in research or clinical practice. Observance of those principles may have protected patients' privacy to the extent that professionals understood and observed them and were, in turn, trusted. Information privacy laws are designed to govern all uses of personal and health information, whether by professionals with traditions of trustworthiness or others. The laws apply regardless, and add formal and inflexible requirements. A reasonable minimum expectation of such laws would be that the protection of the privacy of health information of every Australian was uniform. Neither the scope nor the mechanisms of that protection should vary according to where Australians live or where their health information is held. Where that protection is imposed by different federal and state laws, there is more law than citizens need to protect their privacy. A single well defined system of health privacy protection that achieves a socially acceptable balance between personal control and public benefit is urgently needed.

That the nation simply must do better has been recognised in two recent reports of reviews of the Commonwealth Privacy Act.[13,14] Both reports recommend that the Australian Government undertake a wider comprehensive review of privacy regulation in Australia to ensure that the legislation best serves the needs of Australia in the 21st century. Both reports recognise the inconsistency of regulation, and recommend establishing a nationally consistent privacy protection system, a single set of privacy principles and, in relation to health information, that the Australian Health Ministers' Advisory Council finalise the National Health Privacy Code. The Senate Committee report also recommends that, as part of the wider review of the Privacy Act, the government determine, with appropriate consultation and public debate, what is the appropriate balance between facilitating medical research for public benefit and individual privacy and the right of consent.[14]

Competing interests

None identified.

References

1 *Health Records (Privacy and Access) Act 1997* (ACT).
2 *Information Act 2002* (NT).
3 *Health Records and Information Privacy Act 2002* (NSW).
4 *Health Records Act 2001* (Vic).
5 *Privacy Act 1988*, s. 6 (Cwlth).
6 *Privacy Act 1988*, s. 6C (Cwlth).
7 *Health Records and Information Privacy Act 2002*, s. 4 (NSW).
8 *Information Act 2002*, s. 5 (NT).
9 *Health Records Act 2001*, s. 3 (Vic).
10 *Information Privacy Act 2000* (Vic).
11 *Health Services Act 1991* (Qld).
12 *Privacy and Personal Information Protection Act 1998* (NSW).
13 Office of the Federal Privacy Commissioner. Getting in on the act: the review of the private sector provision of the Privacy Act 1988. March 2005. Available at: http://www.privacy.gov.au/act/review/review2005.htm (accessed Aug 2005).
14 Legal and Constitutional Affairs Committee, Senate, Parliament of Australia. The real Big Brother: inquiry into the Privacy Act 1988. 23 June 2005. Available at: http://www.aph.gov.au/senate/committee/legcon_ctte/privacy/report/ (accessed Aug 2005).

(Received 20 Apr 2005, accepted 18 Jul 2005) ❑