

PRIVACY, CONFIDENTIALITY AND OTHER LEGAL RESPONSIBILITIES

12

Sally Cameron

Australian Federation of AIDS Organisations, NSW.

Note: This chapter refers to a number of key Australian laws and policies relating to privacy, confidentiality and duty of care, and includes a summary of significant legal cases. Although addressing some important questions, this information does not constitute legal advice. In some instances, legislation has been summarised. Practitioners faced with uncertainty in this area are strongly advised to contact their local health department, or the applicable privacy office and they should seek independent legal advice.

This chapter has been adapted from:

Australasian Society for HIV Medicine (ASHM). Australasian Contact Tracing Manual. Edition 3 2006. Canberra: Commonwealth of Australia, 2006: 48-51.

Available at: <http://www.ashm.org.au/contact-tracing/>

Links to: Chapter 11: Infection control and occupational health

KEY POINTS

- Many people are extremely sensitive about the collection and use of information related to their health and health-related treatment.
- Health care practitioners should generally only collect health information about a patient with that patient's informed consent, and should advise the patient of the potential uses of that information.
- Health care practitioners should have sophisticated systems in place governing the storage and access to health information records, including physical and technological security controls, and staff training. This is particularly important for those venues where multi-disciplinary care by different treating practitioners and allied staff may occur.
- *The Privacy Act 1988 (Commonwealth)* (subsequently referred to as 'the Privacy Act') is the primary piece of legislation governing the privacy of health care information in Australia. State and Territory governments also have laws and regulations affecting privacy practices, which may intersect or overlap with the Privacy Act. Health care practitioners must make themselves aware of their privacy and confidentiality obligations in their respective situations.
- Hepatitis B virus infection is a notifiable disease in every Australian State and Territory. Notification does not legally breach a patient's right to privacy, although patients should be informed that notification will occur.
- In Australia, it is illegal to discriminate against a person on the basis of their perceived hepatitis B virus infection or their perceived human immunodeficiency virus (HIV) infection.

Why is privacy and confidentiality important?

The Australian Medical Association (AMA) Code of Ethics requires medical practitioners to maintain a patient's confidentiality. 'Exceptions

to this must be taken very seriously. They may include where there is a serious risk to the patient or another person, where required by law, or where there are overwhelming societal interests.'

In Australia, the protection of health-related information has attracted special treatment, partly as a response to many people considering health information to be extremely sensitive. This point cannot be overemphasised. Most enquiries to the Office of the Privacy Commissioner are from the health sector, and the health sector is second only to the finance sector in the number of complaints received.

While the terms 'privacy' and 'confidentiality' are commonly used interchangeably, they are not identical concepts. Privacy laws regulate the handling of personal information (including health information) through enforceable privacy principles. On the other hand, the legal duty of confidentiality obliges health care practitioners to protect their patients against the inappropriate disclosure of personal (health) information.

It is important to maintain privacy and confidentiality because:

- Patients are concerned about the stigma and discrimination associated with their hepatitis B virus (HBV) status and related conditions
- Patients want to know that they can choose who has access to information about them
- Patients are far more likely to seek medical care and give full and honest accounts of their symptoms if they feel comfortable, respected and secure
- A health system with strong privacy mechanisms will promote public confidence and trust in health care services generally.

Legal requirements

There are no nationally agreed laws or guidelines specifically relating to the diagnosis, treatment and tracing of contacts of patients with HBV or other notifiable diseases. Australian States and Territories have approached the issue differently. Some jurisdictions have gone to great lengths to develop specific, targeted laws and policies, while others have relied on more generic laws and processes. (Please refer to the ASHM Viral Hepatitis Models of Care database available on the ASHM website at www.ashm.org.au/hbv-moc/). However, issues relating to the management of privacy in the health sector are usually covered by the

Privacy Act, which applies to all private sector organisations that provide health services and hold health information. In summary, a 'health service' can be broadly defined as including any activity that involves:

- Assessing, recording, maintaining or improving a person's health; or
- Diagnosing or treating a person's illness or disability; or
- Dispensing a prescription drug or a medicinal preparation by a pharmacist.

Consequently, health services include traditional health service providers, such as private hospitals and day surgeries, medical practitioners, pharmacists and allied health professionals, as well as complementary therapists, gyms, weight loss clinics and many others.

In general terms, the Privacy Act covers all those in the health sector (such as medical practitioners, nurses, administrators, trainers and cleaners) not directly employed by State or Territory governments (as they are usually covered by State laws). Further information on the jurisdiction of the Act is available at http://www.privacy.gov.au/publications/hg_01.html#a2.

The Privacy Act contains 10 National Privacy Principles (NPPs) (available at <http://www.privacy.gov.au/publications/npps01.html>), which govern the minimum privacy standards for handling personal information. Some NPPs state that health service professionals must meet certain obligations, while other NPPs require that they 'take reasonable steps' to meet stated obligations. Practitioners should familiarise themselves with the National Privacy Principles (which are legally binding), and seek advice if necessary.

The different layers of Federal, State and Territory laws and regulations do, in some instances, complicate privacy obligations. In most cases, the privacy protections required by Commonwealth and State or Territory privacy laws are similar. Under the Australian Constitution, when a State/Territory law is inconsistent with a Commonwealth law, the

Commonwealth law prevails. Consequently, across Australia, all private sector health service providers are required to comply with the provisions of the Commonwealth Privacy Act as well as any State/Territory laws.

In NSW, for example, State privacy legislation (the *Health Records and Information Privacy Act 2002*) applies to public sector, and private sector health care providers and holders of health records located in NSW. Consequently, private sector health service providers must comply with two sets of privacy legislation (Federal and NSW), which are largely, but not wholly, compatible. The two sets of legislation impose similar obligations on private health care providers. However, it could be argued that the NSW legislation has a higher compliance threshold, so that if a health care practitioner complies with the NSW *Health Records and Information Privacy Act*, they will generally also comply with the Federal Act (although the two sets of legislation have different enforcement regimes).

Most States now have laws severely restricting the transfer of information in the health sector, and in some States, breaches of confidentiality amount to a criminal offence. In addition to these intersecting laws, many States also have multiple layers of regulation. For example, Queensland Health's Privacy Plan points out that in addition to any relevant Commonwealth and Queensland laws, 'Queensland Health has developed a number of policies related to the management of information at Corporate Office, Directorate, District, facility and unit levels'.

A brief overview of State and Territory privacy laws (and their intersection with the Federal Privacy Act) is provided by The Office of the Privacy Commissioner at http://www.privacy.gov.au/privacy_rights/laws/index.html#1, but for those wishing to seek specific advice (not to be confused with 'legal advice'), the following agencies can be contacted:

All States obligations under the Privacy Act 1988 (Commonwealth)

The Office of the Privacy Commissioner

Tel: 1300 363 992

Email: privacy@privacy.gov.au

State and Territory specific obligations

▪ Australian Capital Territory

The Office of the Privacy Commissioner

Tel: 1300 363 992

Email: privacy@privacy.gov.au

▪ New South Wales

Privacy NSW (Office of the NSW Privacy Commissioner)

Tel: (02) 8688 8585

Email: privacy_nsw@agd.nsw.gov.au

▪ Northern Territory

The Centre for Disease Control

Tel: (08) 8922 8044

The Department of Health and Community Services

Tel: (08) 8922 7049

Email: infoprivacy@nt.gov.au

▪ Queensland

Queensland Health

Tel: (07) 3235 9051

Email: privacy@health.qld.gov.au

▪ South Australia

The Privacy Committee of South Australia

Tel: (08) 8204 8786

Email: privacy@saugov.sa.gov.au

▪ Tasmania

The Office of the Ombudsman

Tel: 1800 001 170

Email: ombudsman@justice.tas.gov.au

▪ Victoria

The Office of the Health Services Commissioner

Tel: 1800 136 066

Email: hsc@dhs.vic.gov.au

▪ Western Australia

The Office of the Information Commissioner

Tel: 1800 621 244

Email: info@foi.wa.gov.au

Privacy issues

There are a number of broad privacy-related issues that face general practitioners and other primary health care providers. These include:

▪ Collecting information

Normally, general practitioners should only collect health information about patients with their consent. It is usually reasonable to assume that consent is implied if the information is noted from details provided by the patient during a consultation, as long as it is clear that the patient understands what information is being recorded and why. It is also vital to ensure that record keeping is thorough and accurate: both to ensure the best-possible ongoing treatment of a patient and, in the worst-case scenario, to be used as defence if a case is made against a treating doctor.

▪ Ensuring consent is 'informed'

All medical procedures require informed consent. Given that the consequences of being tested may be substantial, it is important to realise that, while running tests may be standard for the health care practitioner, receiving the results may be anything but routine for the patient. The provision of information should allow the health care practitioner to discuss the risks and benefits to the patient in their particular situation, thereby facilitating their decision-making process.

▪ Advising use

Patients are not able to consent to the use of their information if they are unclear where the information will go and why. If possible, patients should be advised of the use of their information when it is collected, which can occur through usual communication during a regular consultation. This point also relates to instances when personal information cannot be shared or disclosed. In a recent legal case, a doctor failed to inform two patients attending a joint consultation that the results of each person's test could not be disclosed to the other person, and consequently failed to seek either their understanding of that situation or their consent for their test results to be shared. Please refer to ASHM Viral Hepatitis Models of Care Models of Care database for a summary of relevant case law (available at www.ashm.org.au/hvb-moc/).

▪ Notification

It might be argued that reporting details of a patient's health status involves breaching his or her privacy, however, this practice is legal because there is no 'absolute' right to privacy under Australian or international law. The Privacy Act provides exceptions to privacy where use or disclosure is required by law. In developing Australian privacy laws, the right to individual privacy has been weighed against the rights of others and against matters that benefit society as a whole.

HBV is a notifiable disease in all Australian States and Territories. Legal obligations around notification are mandated by State laws, which define a doctor's duty to notify the respective Health Department of a notifiable disease. In NSW, for example, the Public Health Act 1991 requires doctors to notify their local Public Health Unit by phone or mail of any cases of acute viral hepatitis. Notifications are not to be made by facsimile, in order to protect patient confidentiality. Doctor and hospital notification forms are available at <http://www.health.nsw.gov.au/public-health/forms>.

▪ Accessing personal records

Patients are entitled to access their health records, except for a limited number of important exceptions outlined under NPP 6, for example if the request for access is frivolous or vexatious, or providing access would be likely to prejudice an investigation of possible unlawful activity. The full list of NPP 6 exceptions are listed at <http://www.privacy.gov.au/publications/npps01.html#npp6>. The Office of the Privacy Commissioner's fact sheet relating to access is available at http://www.privacy.gov.au/publications/IS4_01.html.

Patients, including an index case (original person identified with an infection) or a contact, are not entitled to any information that relates to their contact's identity, behaviour or diagnosis without that person's consent, even if that information is in the patient's records. Should a patient wish to access their own record, details of the identity of any contacts contained in their record should be deleted.

▪ Security and storage of health information

A range of laws apply to the storage of health information. Health agencies should have in place:

- Procedures to give access to information only to those people who are authorised to have access in order to use or disclose the information
- Security measures to prevent unauthorised access to the records
- Procedures for storing the information, where practical, in a way that the identity of the person is not readily apparent from the face of the record, e.g. by the use of identification codes
- Procedures for destroying the records that protect the privacy of the information.

Electronic records pose new challenges. While they offer greater convenience of data retrieval and transfer, electronic record systems also create greater risks of data leakage, access by unauthorised staff and 'browsing' by unauthorised people. Agencies and businesses, including medical practices need to consider the security of their data storage and transfer systems and the problem of staff intentionally or inadvertently accessing prohibited electronic records. This issue is currently being addressed by the Commonwealth and a number of States in the development of their electronic health records systems, and has proven enormously complex to date.

▪ Information for teams

Multidisciplinary treating teams are common practice in Australian health care. Health care practitioners work together and share necessary information to deliver optimum health care. All transfers of information without the knowledge of the patient require careful ethical consideration.

Although the question has not yet been legally tested, private sector health service providers do not always require a patient's consent to disclose specific health information to another member of a multidisciplinary team for a health care purpose, as long as the patient would reasonably expect that disclosure. Therefore, it is advisable to tell a patient being treated by a

multidisciplinary team how this will affect the handling of their health information. It is also advisable to gain patient consent to avoid relying on implied consent. Other limited exceptions under NPP 2 permit disclosure without consent in certain circumstances, including to lessen a serious and imminent threat to an individual's life, health or safety; or where the disclosure is required or authorised by law.

There is a need for doctors in group practices to formulate clear internal communication protocols in order to exercise reasonable care, for example, when communicating test results or considering contact tracing issues. The cross-referencing of files per se will generally not breach statutory confidentiality because results need to be checked, though information should not be disclosed without explicit permission. It is vital that all staff are aware of their obligations and that systems are in place for protecting patient privacy.

Exemptions to privacy and confidentiality obligations

The use and disclosure of health information is defined in the Privacy Act under NPP 2 (available at <http://www.privacy.gov.au/publications/npps01.html#npp2>), which states that an organisation must not use or disclose personal information about an individual for a purpose other than the primary purpose of collection, except for a number of situations, including where an organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious and imminent threat to a person's life, health or safety, or a serious threat to public health or public safety.

In short, health care workers must not disclose a person's health information except in a very limited number of circumstances. These may generally be summarised as:

- Communicating necessary information to others directly involved in the treatment of a patient during a particular episode of care
- Cases of needlestick injury where a professional is aware of a patient's HBV positive status, and a health care worker has been exposed to circumstances where there is a real risk of transmission and it is

not possible to conceal the identity of the source patient who has refused to consent to disclosure

- Provision of medical services in a particular instance of care where there is a need to know the patient's infection status for treatment purposes of benefit to the patient (e.g. in an emergency or if the patient is unconscious). This should not, however, detract from the observance of standard infection control precautions.

It is strongly recommended that practitioners familiarise themselves with the National Privacy Principles (which are legally binding) and contact the Office of the Privacy Commissioner if they wish to clarify the manner in which the National Privacy Principles might relate to specific situations. Legal advice should be sought from a legal practitioner.

Contact tracing

The practice of contact tracing raises the question of potential conflict between breaching a patient's privacy and confidentiality, and alerting a third party to the fact that they may be at risk of HBV infection. Although a case on this specific point is yet to be heard in Australia, it seems likely that a health practitioner could be found negligent to a third party if they did not warn the third party that they were at risk. This potential conflict may be further complicated by a statutory obligation to counsel patients regarding sexually transmissible medical conditions.

Fortunately, public health services afford practitioners expert guidance to resolve the conflict between the duties to maintain confidentiality and privacy, and a possible duty of care owed to third parties. In instances where practitioners suspect a person may be putting others at risk, the practitioner should notify the health department using the methods prescribed by the relevant State or Territory. Public health authorities then become responsible for making decisions around contact tracing, including the management of privacy issues. For a more detailed account of the contact tracing responsibilities of health care providers, please consult the *Australasian Contact Tracing Manual Ed 3*, available at: <http://www.ashm.org.au/contact-tracing/>.

Criminal law

There are two types of criminal offences associated with HBV and other blood-borne viruses. The first relates to the disclosure of information regarding a person who has an infection, or is suspected of having HBV or other blood-borne virus infections—as discussed above. There are also laws in every State and Territory making it an offence to transmit an infection to another person. As with other areas of legislation, specifications around definition and scope differ across jurisdictions. The majority of these laws are not specific to blood-borne viruses, but instead refer to infectious diseases generally; more generic criminal offences, for example, causing grievous bodily harm, may also be applied.

Anti-discrimination

Anti-discrimination provisions exist across all Australian States and Territories, making it illegal to discriminate against people on the basis of their (perceived) HBV infection. Discrimination is prohibited on the basis of disability or impairment. It is important that health care practitioners consider behaviours they must avoid when testing and managing people with HBV. Discrimination on the basis of disability or impairment includes treating a person less favourably as a result of their (perceived) disability or impairment. In a health care setting, this may include refusing to see a patient, offering different or inappropriate treatment, or placing a patient last on a consultation or operating list. As outlined in Chapter 11: Infection control and occupational health, standard precautions ensure a high level of protection against the transmission of infection in the health care setting and represent the level of infection control required in the treatment and care of all patients to prevent transmission of blood-borne infections.

Health care workers with HBV infection

Please refer to Chapter 11: Infection control and occupational health for obligations of health care practitioners who perform exposure prone procedures.