Introduction and key concepts

Contents

Who should read this guide?

This guide is written to help health service providers comply with their existing obligations under the *Privacy Act 1988* (Privacy Act). It should be read in conjunction with the Privacy Act and the Australian Privacy Principles (APP) Guidelines.

Health service providers range from doctors and private sector hospitals, through to allied health professionals, complementary medicine practitioners, pharmacists, private schools and childcare centres, gyms and weight loss clinics.

Health service providers constantly handle health information about their patients and understand that health information is sensitive in nature and needs to be treated carefully. Handling this information appropriately underpins the trust in a provider-patient relationship.

The guide outlines the key practical steps that health service providers should take to embed good privacy in their practice. In addition, the guide outlines how key privacy obligations apply to and operate in the healthcare context.

Taking these key practical steps and understanding your privacy obligations will enable you to identify and implement practices that reduce privacy risk and generate public trust in your handling of individuals' health information.

Key concepts

Collection

Collection means gathering, acquiring or obtaining personal information for inclusion in a record or generally available publication. In practice, you collect health information about a patient if you receive health information from the patient, or from another source, and you retain it.

Examples of collection include:

- recording what a patient says, or recording your opinion about what a patient has said
- requiring a patient to complete a form requesting details such as name, address, date of birth and medical history
- keeping a specialist report provided by a patient for inclusion in the patient's medical record
- taking physical or biological samples from a patient and labelling these with the patient's name or other identifier
- storing video footage, photographs or audio recordings in which a patient can be reasonably identified
- keeping emails or other correspondence containing personal information about a patient.

Competent health or medical bodies

The Privacy Act does not specify which bodies are 'competent health or medical bodies'. Examples could include medical boards and other rule-making bodies recognised in an applicable Australian law.

Consent

Consent can be either express or implied. Express consent is given explicitly, either orally or in writing by an affirmative, unambiguous act. Implied consent arises where you can infer from the circumstances, and the conduct of the patient, that consent is being given to the handling of the health information.

The key elements of consent are:

- the individual is adequately informed before giving consent
- the individual gives consent voluntarily
- the individual has the capacity to understand and communicate consent
- the consent is current and
- the consent is specific.

Consent, as discussed in this guide, applies to a patient's decisions about how you handle the patient's health information. It does not refer to consent to receiving treatment. In practice, consent to the handling of health information and consent to treatment often occur at the same time, though they are distinct authorities by a patient to different things.

Chapter B: Key concepts of the APP Guidelines contains a more detailed discussion of 'consent'.

De-identify and de-identification

Personal information is de-identified once the information is no longer about an identifiable individual or an individual who is reasonably identifiable. De-identified information is not 'personal information'.

Generally, de-identification includes two steps:

- removing personal identifiers, such as name, address, date of birth or other identifying information, and
- removing or altering other information that may allow an individual to be identified, for example, because of a rare characteristic of the individual, or a combination of unique or remarkable characteristics that enable identification.

De-identification may not altogether remove the risk that an individual can be re-identified. There may, for example, be a possibility that another dataset or other information could be matched with the de-identified information. The risk of re-identification must be actively assessed and managed to mitigate this risk. Relevant factors to consider when determining whether information has been effectively de-identified could include the cost, difficulty, practicality and likelihood of re-identification.

For further information on how to de-identify information, and how to manage and mitigate the risk of re-identification, see De-identification and the Privacy Act.

Disclosure

You disclose health information when you make it accessible to others outside your organisation and you release the subsequent handling of that information from your effective control. This includes giving health information to a related body corporate.

Examples of disclosure include:

- sharing health information with another health service provider or individual
- providing health information to an unintended recipient
- displaying a computer screen so that health information can be read by someone else, for example, at a reception counter or in an office.

Health service and health service providers

'Health service' means:

- an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or person performing it:
  - to assess, maintain or improve the individual's health
  - where the individual's health cannot be maintained or improved — to manage the individual's health
  - to diagnose the individual's illness, disability or injury
  - to treat the individual's illness, disability or injury or suspected illness, disability or injury

  - to record the individual's health for the purpose of assessing, maintaining, improving or managing the individual's health
- the dispensing on prescription of a drug or medicinal preparation by a pharmacist.

These activities include those taking place in the course of providing aged care, palliative care or care for a person with a disability.

Some examples of health service providers covered by the Privacy Act include:

- general practitioners and medical specialists
- private hospitals and day procedure centres
- pharmacists
- other health and allied health professionals such as psychologists, dentists, physiotherapists, podiatrists, occupational and speech therapists, optometrists and audiologists
- private aged care and palliative care facilities
- pathology and radiology services
- complementary medicine practitioners, including herbalists, naturopaths, chiropractors, massage therapists, nutritionists, and traditional Chinese medicine practitioners
- health services provided in the non-government sector, such as phone counselling services or drug and alcohol services
- private schools and childcare centres
- disability service providers (where they handle health information)
- gyms and weight loss clinics
- blood and tissue banks
- assisted fertility and IVF clinics
- health services provided via the Internet (eg counselling, advice, medicines), telehealth and health mail order companies.

Health information

All personal information collected in the course of providing a health service is considered health information under the Privacy Act. Health information is 'sensitive information' under the Privacy Act, meaning that some stricter requirements apply when handling it.

'Health information' means:

- information or an opinion about:
  - the health, including an illness, disability or injury, (at any time) of an individual
  - an individual's expressed wishes about the future provision of health services to him or her
  - a health service provided, or to be provided, to an individual

  that is also personal information
- other personal information collected to provide, or in providing a health service to an individual. This includes personal details such as a patient's name, address, admission and discharge dates, billing information and Medicare number

- other personal information collected in connection with the donation, or intended donation, by an individual of his or her body parts, organs or body substances
- genetic information about an individual in a form that is, or could be, predictive of the health of that individual or a genetic relative of the individual.

Examples of health information include:

- information about an individual's physical or mental health
- notes of an individual's symptoms or diagnosis and the treatment given
- specialist reports and test results
- physical or biological samples where they could be linked to a patient (for example where labelled with the patient's name or other identifier)
- appointment and billing details
- prescriptions and other pharmaceutical purchases
- dental records
- records held by a fitness club about an individual
- an individual's healthcare identifier when it is collected to provide a health service
- any other personal information (such as information about an individual's date of birth, gender, race, sexuality or religion), collected for the purpose of providing a health service.

Genetic information

Genetic information is 'sensitive information' under the Privacy Act, meaning that some stricter requirements apply when handling it. Genetic information that is 'about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual' is also considered health information.

Responsible person

Where a patient is a child or lacks physical and/or mental capacity, information about the patient can, in certain circumstances, be collected from or disclosed to a 'responsible person'. A 'responsible person' for a patient includes:

- a parent of the patient
- a child or sibling of the patient (who is at least 18 years old)
- spouse or de facto partner of the patient
- a patient's relative (if the relative is over 18 years old and part of the patient's household)
- the patient's guardian
- a person exercising an enduring power of attorney granted by the patient that is exercisable in relation to decisions about the patient's health
- a person who has an intimate personal relationship with the patient or
- a person nominated by the patient to be contacted in the case of emergency.

'Responsible person' includes step relationships, in-laws, adopted relationships, foster relationships and half-brothers and sisters.

Serious threat

A 'serious' threat is one that poses a significant danger to an individual or individuals. This can include a threat to a patient's physical or mental health and safety. It can also include a potentially life threatening situation or one that might reasonably result in other serious injury or illness. The threat may be to the life, health or safety of any individual and is not limited to a person seeking treatment and care.

A 'serious threat to public health or safety' relates to broader concerns affecting a number of people. An example is the potential spread of a communicable disease.

When deciding whether a threat is serious, you should consider both the likelihood of it occurring and the severity of the resulting harm if it eventuates. A threat that may have dire consequences but is highly unlikely to occur would not normally be a serious threat. However, a potentially harmful threat that is likely to occur, but at an uncertain time, may be a serious threat.

Use

Generally, you use health information where you handle, manage or undertake an activity with that information within your effective control. Examples of uses include:

- accessing and reading a patient's medical file
- searching electronic records for a patient's health information
- making a treatment decision based on a patient's health information
- passing the information from one part of your organisation to another.