Australian Government

Office of the Australian Information Commissioner

Guide to health privacy

oaic.gov.au

OAIC

Collated May 2025

Contents

A comprehensive contents page appears at the beginning of each chapter.

Introduction and key concepts

Chapter 1: Key steps to embedding privacy in your health practice

Chapter 2: Collecting health information

Chapter 3: Using or disclosing health information

Chapter 4: Giving access to health information

Chapter 5: Correcting health information

Chapter 6: Health management activities

Chapter 7: Disclosing information about patients with impaired capacity

Chapter 8: Using and disclosing genetic information in the case of a serious threat

Chapter 9: Research

Introduction and key concepts

Contents

Who should read this guide? **1**

Key concepts **2**

Collection 2
Competent health or medical bodies 2
Consent 2
De-identify and de-identification 3
Disclosure 3
Health service and health service providers 3
Health information 4
Genetic information 5
Responsible person 5
Serious threat 6
Use 6

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.

This guide was updated in May 2025, with version 2.0 amendments focussed specifically on Chapter 8: Using and disclosing genetic information in the case of a serious threat.

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.

Chapter 1: Key steps to embedding privacy in your health practice

Contents

Key points 1

Eight key steps 2

Step 1: Develop and implement a privacy management plan 2
Step 2: Develop clear lines of accountability for privacy management 2
Step 3: Create a documented record of the types of personal information you handle 3
Step 4: Understand your privacy obligations and implement processes 3
Step 5: Staff training 4
Step 6: Create an APP privacy policy 4
Step 7: Take reasonable steps to protect and secure personal information 5
Step 8: Develop a data breach response plan 5

Key points

- The *Privacy Act 1988* (Privacy Act) requires you to be proactive in establishing, implementing and maintaining privacy processes in your practice.
- To meet your privacy obligations and to make managing privacy easier, the key practical steps you should take are:

  Develop and implement a privacy management plan

  Develop clear lines of accountability for privacy management

  Create a documented record of the types of personal information you handle

  Understand your privacy obligations and implement processes to meet those obligations

  Hold staff training sessions on privacy obligations

  Create a privacy policy

  Protect the information you hold

  Develop a data breach response plan.

Eight key steps

The Privacy Act requires you to be proactive in establishing, implementing and maintaining privacy processes in your practice.

There are eight key steps you should take which will help you to meet this requirement. This chapter outlines the key steps you should take and provides details and links to further information.

Taking these key steps will help you to meet your privacy obligations, and make it easier to manage privacy within your health practice.

Step 1: Develop and implement a privacy management plan

The Privacy Act requires you to be proactive in establishing, implementing and maintaining privacy processes that ensure you comply with the Australian Privacy Principles (APPs).

The OAIC has developed a Privacy management framework that sets out the four broad steps you are expected to take to meet your obligations:

1. Embed: a culture of privacy that enables compliance
2. Establish: robust and effective privacy processes
3. Evaluate: your privacy processes to ensure continued effectiveness
4. Enhance: your response to privacy issues.

A key tool for meeting your obligations is to develop and implement a 'privacy management plan' that aligns your practice's business processes with your privacy obligations. A privacy management plan is a document that identifies specific and measurable privacy goals and targets to help you implement these four steps.

For more information, see the OAIC's Privacy management plan template, which is designed to help you develop a privacy management plan.

Step 2: Develop clear lines of accountability for privacy management

Your practice should have clear lines of accountability for managing privacy issues.

Knowing whom in the practice has the expertise and responsibility for meeting privacy requirements helps all staff respond efficiently to any privacy issues and seek prompt guidance when they need it.

For example, if the practice manager is responsible for privacy management, this should be clearly communicated to all staff and the practice manager should be accessible to answer any queries or to assist staff to better understand how the practice manages privacy.

Alternatively, in a larger healthcare practice — such as a private hospital — a number of staff members with particular expertise in privacy or, more broadly, regulatory requirements, might be designated privacy officers. These privacy officers can act as centralised points of contact for other staff to approach in the event that:

- they have any questions or require advice about how to handle personal information and related compliance obligations
- they need assistance in responding to a privacy-related complaint or query from a patient
- a privacy incident occurs, such as a data breach, which needs to be addressed promptly.

Step 3: Create a documented record of the types of personal information you handle

Understanding your practice's personal information holdings is an important foundation for effective privacy management and compliance.

Understanding the personal information holdings means understanding:

- **types of personal information handled**: examples include clinical notes, general patient information including contact information and Medicare/healthcare fund details, specialist reports, test results, imaging films, referral letters
- **how personal information is received**: examples include records generated within your practice, and written and verbal information from patients, other healthcare providers, insurers and lawyers
- **where personal information is held**: consider all physical and electronic records within your control, including at your premises, off-site physical locations, and cloud storage providers.

Having a thorough and documented record of the personal information you handle will help you to:

- develop a privacy policy (which must include the personal information you collect and hold)
- consider how best to protect and secure that information
- confidently and efficiently provide individuals with access to their personal information
- assess the purposes for which you can use or disclose the information consistently with your privacy obligations.

Step 4: Understand your privacy obligations and implement processes

It is important to gain an understanding of your privacy obligations.

While Chapter 1 outlines the key practical steps you should take to embed good privacy governance in your practice, the remaining chapters of this guide look in more detail at how key APPs apply to and operate in a healthcare context.

Once you understand your privacy obligations, you should develop and implement processes that facilitate your practice's compliance with those obligations.

These processes should:

- address the handling of information throughout the information life cycle — that is, consider the handling from collection, through various uses and disclosure of the information, to storage and security, and to when the information is no longer required
- clearly outline how staff are expected to handle personal information in their everyday roles

- include processes to allow individuals to easily access and correct their personal information
- include processes for receiving and responding to patients' privacy enquires and complaints.

Step 5: Staff training

Training staff on their privacy obligations and the importance of privacy will help to create a confident team that is able to handle personal information in a privacy enhancing way.

Examples of activities that can facilitate a privacy-aware culture within your practice include:

- running training for all new staff that includes information on privacy requirements and the practice's current privacy practices and expectations
- developing clear and consistent processes for staff to follow to ensure everyone is aware of their obligations and who to ask for assistance
- making privacy-related resources accessible to staff via email or, for example, by posting them on a staff intranet
- holding information sessions on emerging privacy issues or risks, developments that impact how personal information is handled, or privacy breaches or complaints that have occurred
- encouraging and facilitating professional development opportunities for staff whose role needs a deeper understanding of privacy or security.

Step 6: Create an APP privacy policy

The Privacy Act requires you to have a clearly expressed and up-to-date privacy policy which describes how you manage personal information.

Your privacy policy must cover:

- the kinds of personal information you collect and hold
- how you collect and hold personal information
- the purposes for which you collect, hold, use and disclose personal information
- how an individual may access personal information and seek its correction
- how an individual may complain if you breach the Privacy Act and how the complaint will be handled
- whether you are likely to disclose personal information to overseas recipients, and if so, the countries in which such recipients are likely to be located.

You must take reasonable steps to make the privacy policy available free of charge and in an appropriate format. This might include making the policy available on your website, or prominently displaying a copy of the policy (or instructions for how to obtain it) in your practice. If a patient asks for the policy in a particular format, you should give the individual the policy in that format.

For further information and assistance in developing a privacy policy, see the OAIC's Guide to developing an APP privacy policy and Chapter 1 of the APP Guidelines.

Step 7: Take reasonable steps to protect and secure personal information

The Privacy Act requires you to take reasonable steps to:

- protect the personal information you hold from misuse, interference, loss, and from unauthorised access, modification or disclosure
- destroy or de-identify personal information you hold once it is no longer needed.

Reasonable steps should include, where relevant, taking steps and implementing strategies in relation to the following:

- governance, culture and training
- internal practices, procedures and systems
- ICT security
- access security
- third party providers (including cloud computing)
- data breaches
- physical security
- destruction and de-identification
- standards.

For further information, see the OAIC's Guide to securing personal information.

Step 8: Develop a data breach response plan

Developing a data breach response plan is another reasonable step you can take to protect and secure personal information you hold.

A data breach is when personal information is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference. Examples of a data breach are when:

- a device containing personal information of clients is lost or stolen
- an entity's database containing personal information is hacked
- an entity mistakenly provides personal information to the wrong person.

A data breach response plan is a tool to help you manage a data breach. It is a framework setting out how you will manage and respond to a data breach, including the steps you will take and the roles of various staff members. Having a data breach response plan enables you to act quickly and effectively in the event a breach occurs.

To assist you in developing a data breach response plan, the OAIC has developed a guide to preparing a data breach response plan.

Your data breach response plan should also address notification obligations:

- You will need to notify the Australian Information Commissioner and affected individuals in the case of a breach involving personal information that is likely to result in serious harm to any affected individual.

- You will need to notify the Information Commissioner and the System Operator in the case of breaches of information held in the My Health Record system.

For further information on your data breach notification obligations, see the OAIC's Notifiable Data Breaches webpage and the OAIC's Guide to mandatory data breach notification in the My Health Record system.

Chapter 2: Collecting health information

Contents

Key points 1

Collecting health information 2

How should you collect health information? 2

Directly from the patient 2

By lawful and fair means 2

Notifying patients of collection (privacy notices) 3

When should you provide notice? 3

What must you include in a privacy notice? 3

How do you provide notice? 4

Collecting health information without consent 5

Required or authorised by law 5

Serious threat 5

Providing a health service 6

Medical history-taking 6

Conducting research; compiling or analysing statistics; management, funding or monitoring of a health service 6

Other situations 6

Anonymity and pseudonymity 7

Unsolicited health information 7

Key points

- With your patients' consent, you can collect their health information when it is reasonably necessary for your activities.
- You must only collect health information by lawful and fair means, and generally only directly from the patient.
- You must take reasonable steps to notify the patient of certain matters when you collect health information.

Collecting health information

You can collect health information about a patient if:

- the patient consents (expressly or impliedly) to you collecting it, and
- the information is *reasonably necessary* for your activities (which would generally be providing a health service to that patient).[1]

Example: Implied consent to collection

During a consultation, a patient describes his symptoms and provides you with his medical history. You add this information to the patient's record on your system. From the patient's conduct in this situation, you can imply the patient's consent to you collecting his health information.

How should you collect health information?

Directly from the patient

You must only collect health information about a patient directly from the patient, unless it is not reasonable or practical to do so.

Whether collecting directly from the patient is reasonable and practicable depends on a number of factors, including the nature of the information and accepted practice in the health sector.

Examples of where collecting health information directly from a patient may not be reasonable or practical include:

- in an emergency you may need to collect the patient's background health information from relatives
- where a patient is a child, or an adult who lacks capacity, you may need to collect the information from parents, guardians or relatives, or
- where a pathologist collects a specimen and related information from a referring provider.

By lawful and fair means

You must only collect health information by lawful and fair means.

'Lawful' collection is a collection that does not breach any State, Territory or Commonwealth law.

'Fair means' is collecting without intimidation or deception, and in a way that is not unreasonably intrusive.

[1] Note that under the *My Health Records Act 2012* more specific requirements apply to the collection of health information relating to the My Health Record system. Similarly, the *Healthcare Identifiers Act 2010* has particular requirements for the collection of healthcare identifiers.

Example: Unlawful collection

Under the *Telecommunications (Interception) Act 1979* (Cth) and State and Territory listening devices laws, it is illegal to record a telephone consultation without informing the patient the call is being recorded. Collection via this method would therefore not be by lawful means. If a call is to be recorded or monitored, you must inform the individual at the beginning of the conversation so that the individual has a chance to end the call or ask not to be recorded.

Example: Intrusive collection

Patients may be concerned or embarrassed about discussing health issues in an open or public area such as a waiting room or open pharmacy. When collecting health information, you should consider the surroundings and take additional steps where required to make the patient more comfortable. For example, you might lower your voice so only the patient can hear what you are saying, take the patient to one side, or use a private room.

Notifying patients of collection (privacy notices)

When you collect a patient's health information, you must take reasonable steps to notify the patient of certain matters. Providing this notice ensures the patient understands why the information is being collected and how it will be handled.

When should you provide notice?

Generally, you should give this notice before or at the time of collection. This allows a patient to make an informed choice about whether to provide the health information.

If that is not practicable, you should give notice as soon as practicable afterwards. For example, in a medical emergency, there is unlikely to be time to provide notice or the individual may not be in a fit state to comprehend the information. In this case, you should notify the patient of the matters as soon as practical after you provide the health service.

What must you include in a privacy notice?

The matters to include in your privacy notice are:

- your organisation's identity and contact details
- if the patient may not be aware of the collection (including where the information is collected from a third party), the fact that you collect the information and the circumstances of collection
- whether the collection is required or authorised by law
- the purposes of collection
- any consequences for the patient if the health information is not collected
- your usual disclosures of the health information you collect

- that your Australian Privacy Principles (APP) privacy policy contains information on:
  - how patients can access and correct the health information you hold about them
  - how patients can make a complaint about how you handle their health information, and details of how you will deal with a complaint
  - whether you are likely to disclose health information overseas (and if so, where).

Helpful hint

As part of notifying patients about your usual disclosures of their health information, it is a good idea to ensure patients are aware of which members of a 'treating team' you will disclose their health information to. This may be a requirement for providers practising in the ACT — contact the ACT Health Services Commissioner to find out more about this requirement.

How do you provide notice?

You are required to take reasonable steps to notify the patient of these matters. What steps are reasonable depends on the circumstances.

Some of the matters may be obvious (such as the identity and contact details of the practice when a patient attends their GP) in which case it may be reasonable to take no steps to notify the patient of those matters. In addition, unless there is a change in information handling practices, you will only need to notify a patient of these matters on the first visit, and it is reasonable to take no notification steps when you collect information on subsequent visits.

Example: Privacy notices

Examples of ways in which you might choose to provide a privacy notice include:

- Prominently displaying a brief notice at the check-in counter covering key information, and giving the individual more detailed notice in a leaflet.
- Including a privacy notice on a paper or online form used to collect patients' health information.
- Discussing the information orally during a consultation with a patient. To ensure all relevant matters are covered, it would be useful to also provide the patient with a written notice in this situation.

For more information, see the APP Guidelines, Chapter 5: APP 5 — Notification of the collection of personal information.

Collecting health information without consent

While you generally need consent to collect a patient's health information, you may collect it without consent in the situations set out below.

Required or authorised by law

You may collect health information without consent where the collection is 'required or authorised by or under an Australian law or a court/tribunal order'.

Example: Law requiring collection

Under State and Territory public health legislation, health service providers are required to record information about individuals with certain diseases and notify the relevant health authority.

For example, under the NSW *Public Health Act 2010*, doctors, hospitals and pathology laboratories are required to record information about patients with certain medical conditions, such as AIDS, malaria, measles, tetanus and typhoid, and notify the NSW Department of Health. To meet your legislative obligations, you can collect relevant health information without the patient's consent.

Serious threat

You may collect health information without consent where it is unreasonable or impracticable to obtain consent to the collection, and you reasonably believe the collection is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety.

You must have a reasonable basis for your belief that there is a serious threat, and you must be able to justify it. The test is what a reasonable person, who is properly informed, would believe in the circumstances.

You cannot avoid obtaining consent just because it would be inconvenient, time-consuming or impose some cost. Whether these factors make it impracticable to obtain consent will depend on whether the burden is excessive in all the circumstances.

Example: Necessary to lessen a serious threat to an unconscious patient

A patient is in hospital and unconscious as a result of a stroke and the hospital needs further information from his GP to determine how best to treat him. Given the patient's condition, it is not practical to obtain his consent to the collection. Further, the hospital reasonably believes that the collection of this information from the GP is necessary to lessen the serious threat to the patient's health. In this situation, the hospital can collect health information without the patient's consent.

Providing a health service

You may collect health information without consent where the information is necessary to provide a health service to a patient, and either:

- the collection is required or authorised by or under an Australian law, or
- it is collected in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which are binding on you.

Medical history-taking

You can collect health information from a patient about another individual, without that individual's consent, where:

- it is part of the patient's family, social or medical history, and
- that history is necessary to provide a health service to the patient.

Examples of information that are part of a patient's family, social or medical history include:

- aspects of the medical history of the patient's family members, such as inheritable conditions
- information about non-family members, such as a household member with a contagious illness
- information about the health of a primary carer of a disabled patient, where the patient advises that the carer is struggling with some aspects of the patient's care due to severe arthritis
- a drug rehabilitation service collecting information about the mental health of a patient's partner.

You should limit the information you collect to that which is necessary to provide the health service to the patient. Information is 'necessary' to provide a health service if you cannot effectively provide the health service without collecting it.

Conducting research; compiling or analysing statistics; management, funding or monitoring of a health service

You may collect health information about an individual if:

- the collection is necessary for research or statistical activities relevant to public health or public safety, or for the management, funding or monitoring of a health service, and
- certain other criteria are met.

If you collect health information in these circumstances and subsequently want to disclose that information, you must take reasonable steps to de-identify the information before disclosing it.

For more information, see Chapter 9.

Other situations

Other situations where you may collect health information without consent include:

- taking appropriate action in relation to suspected unlawful activity or serious misconduct
- locating a person reported as missing

- where it is reasonably necessary for establishing, exercising or defending a legal or equitable claim, or for a confidential alternative dispute resolution process.

For more information, see the APP Guidelines Chapter C: Permitted general situations.

Anonymity and pseudonymity

The *Privacy Act 1988* (Privacy Act) requires you to consider whether it is practical to give patients the option of not identifying themselves, or using a pseudonym, when dealing with you. A patient may prefer to deal anonymously or pseudonymously with a health service provider for various reasons. For example, a patient may wish to access counselling or other services without this information being linked to her identity and potentially becoming known to others.

However, you do not have to deal with patients anonymously or pseudonymously where:

- you are required or authorised under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves, or
- it is not practical for you to deal with unidentified individuals or those using a pseudonym.

While it may often be unlawful or impracticable to provide a health service anonymously or pseudonymously, you should still consider whether there are situations in which you can offer anonymous or pseudonymous healthcare in certain situations and ensure patients are aware of this possibility if applicable. For example, your privacy policy could explain the circumstances in which a patient may deal anonymously or by pseudonym with you, and the procedures for doing so.

There may also be consequences for patients if they do not identify themselves, such as for their ongoing healthcare and their ability to claim a Medicare or health fund rebate.

See the APP Guidelines, Chapter 2: APP 2 — Anonymity and pseudonymity for more information.

Unsolicited health information

Unsolicited health information is information that you come across by accident, or receive but have not requested.

If you receive unsolicited health information you should, within a reasonable period of time, determine whether the Privacy Act would have allowed you to collect the information. As outlined above, you generally would have needed the patient's consent to collect the health information, unless an exception applies. If you could have collected the information, then you must comply with the Privacy Act when handling it.

If you could not have collected the information, then you must destroy or de-identify the health information as soon as practicable if it is lawful and reasonable to do so.

For further information, see the APP Guidelines, Chapter 4: APP 4 — Dealing with unsolicited personal information.

Example: Collecting unsolicited information to lessen a serious threat

The son of an elderly patient sends you an email expressing his concern that your patient is unfit to drive. The son suggests that your patient has caused a number of recent near car accidents. The son claims his Dad is determined to keep driving, and the son says he is worried his Dad may injure himself and others. He provides details of these incidents and there appears to be cause for concern, particularly given the patient's recent medical history. Having received this unsolicited information, you need to consider whether you could have collected this information under the Privacy Act. In this case, you may be able to conclude that you could have collected this information because you reasonably believe the collection is necessary to enable you to take steps to lessen or prevent a serious threat to the health or safety of your patient and other individuals.

Chapter 3: Using or disclosing health information

Contents

Key points 1

Using or disclosing health information 2

Using or disclosing for the primary purpose 2

Using or disclosing for a secondary purpose 3

- Consent 3
- Reasonably expected and directly related 3
- Required or authorised by law 4
- Serious threat 5
- Conducting research, or the compilation or analysis of statistics 5
- Preventing a serious threat to the life, health or safety of a genetic relative 6
- Disclosure to a responsible person for an individual 6
- For enforcement related activities 6
- Other situations 7

Overseas disclosure 7

Direct marketing 7

Government related identifiers 7

Key points

- You can use and disclose a patient's health information for the primary purpose for which you collected it.
- You can use and disclose a patient's health information for another purpose with the patient's consent.
- Otherwise, you can only use and disclose a patient's health information for another purpose in certain circumstances.

Using or disclosing health information

You can use or disclose health information about a patient:

- for the primary purpose for which you collected it, or
- for a secondary purpose in certain circumstances.[1]

Using or disclosing for the primary purpose

You can use or disclose health information about your patients for the 'primary purpose' for which you collected it. The primary purpose is the specific main activity for which you collected the information.

The context in which you collect health information helps to identify the primary purpose of collection. For example, if a patient provides a GP with his health information during a consultation, the primary purpose of the GP collecting his information is to provide general practice services to diagnose and treat that patient.

The intent behind the use and disclosure requirements is to ensure that you only use and disclose a patient's health information in ways the patient would expect. Therefore, if the primary purpose of collection is unclear, you should view it narrowly so that your subsequent uses and disclosures are in line with a patient's expectations.

Helpful hint

State or Territory legislation may place additional requirements on providers in those jurisdictions. For example, providers in the ACT who collect a patient's personal information from another provider for a particular purpose may not be permitted to use or disclose it for a secondary purpose.

Contact the Information and Privacy Commission NSW, Victorian Health Complaints Commissioner, or ACT Health Services Commissioner to find out more about any additional requirements.

[1] More specific requirements apply to the use and disclosure of:

- health information for the purpose of direct marketing
- government-related identifiers that are considered health information
- healthcare identifiers
- health information relating to the My Health Record system.

Using or disclosing for a secondary purpose

Any purpose other than the primary purpose is a secondary purpose. You can only use or disclose a patient's health information for a secondary purpose in the circumstances set out below.

Consent

You can use or disclose health information for a secondary purpose with the patient's consent.

Reasonably expected and directly related

You can use or disclose a patient's health information if:

- the patient would reasonably expect you to use or disclose the information for that purpose, and
- the purpose is directly related to the primary purpose of collection.

A patient's reasonable expectations are what an ordinary person would expect to happen to the health information in the circumstances. This is based on:

- general community expectations of how information usually flows within the health system
- what you tell your patient about how the health information will be handled (both during discussions and in your privacy notice), and the patient's reaction to this information.

Example: Referral to a specialist

When a GP refers a patient to a specialist, most patients would expect the GP to disclose personal health information in the referral letter, and would expect the specialist to disclose information arising from the consultation back to the GP.

This general expectation reflects this common information handling practice in the health system. In addition, GPs and specialists usually advise their patient that they will contact the other practitioner in connection with the referral, and these discussions further inform a patient's reasonable expectation of when you will disclose the health information.

Example: Treating team

A multi-disciplinary team approach to health care is common and usually involves sharing a patient's health information within a 'treating team'. It is important that the patient understands when and what information will be shared within a treating team, and who is part of the team. Once you have discussed this with your patient, there will be a reasonable expectation that health information will be disclosed within the treating team (provided the patient has not expressed concerns), and team members will not need to get the patient's consent to uses and disclosures. If the patient has expressed concern about disclosures to certain team members, then you are likely to need consent to share information with that practitioner.

A directly related secondary purpose is a purpose closely associated with the primary purpose, even if it is not strictly necessary to fulfil that primary purpose. Directly related purposes are likely to include anything to do with the patient's care or wellbeing.

Activities or processes necessary for the functioning of the health sector may also be directly related purposes (see examples below). Provided these purposes are within a patient's reasonable expectations, you do not need to take other steps before use or disclosure. In addition, you should only use or disclose the minimum amount of information necessary to achieve the purpose.

Example: Directly related purposes

- Billing or debt recovery (provided this is done consistently with confidentiality obligations).
- Management, funding, complaint-handling, planning, evaluation and accreditation activities, and quality assurance, incident monitoring or clinical audit activities (although you should consider whether de-identified information can achieve these purposes).
- Disclosure to a medical expert (for a medico-legal opinion), insurer, medical defence organisation, or lawyer, for the purpose of addressing liability indemnity arrangements (such as reporting an adverse incident), legal proceedings, or for the provision of legal advice.
- Disclosure to a clinical supervisor by a psychiatrist, psychologist or social worker.

Example: registration

You are audited for quality assurance as part of being 'vocationally registered' under Medicare. The auditor examines patient records 'on the spot'. This could be a disclosure and there is limited opportunity for you to obtain patient consent. While you originally collected the health information for the primary purpose of providing healthcare, the disclosure for the secondary purpose will be permitted if being vocationally registered is considered directly related to providing healthcare, and if the patient would reasonably expect this disclosure.

Required or authorised by law

You can use or disclose health information where the use or disclosure is required or authorised by or under an Australian law or a court/tribunal order.

If the law *requires* you to use or disclose information, you must do so. Examples include mandatory reporting of child abuse (under care and protection laws) and mandatory notification of certain communicable diseases (under public health laws).

If the law *authorises* you to use or disclose information, you can decide whether to do so or not — the legal authority exists, but you have discretion as to whether to handle information in that way.

Example: required by law

Under s 23DS of the *Health Insurance Act 1973,* a radiologist is required to produce records of diagnostic imaging services upon request by Medicare. Given the legislative requirement, a radiologist can disclose records in this situation without breaching the *Privacy Act 1988* (Privacy Act).

Example: courts and legal proceedings

If you are served with a subpoena or other court order requiring you to produce documents, you are generally required by law to provide those documents. However, you can challenge court orders in some situations and you may not be required to produce all the documents you hold (such as where you can claim legal professional privilege over a legal advice prepared for you by a lawyer).

If you are concerned or unsure about how to proceed, you could seek advice via the registrar of the issuing court or tribunal, a legal adviser, your professional body or your indemnity insurer.

Serious threat

You can use or disclose health information where it is unreasonable or impracticable to obtain consent to the use or disclosure, and you reasonably believe the use or disclosure is necessary to lessen or prevent a **serious threat** to the life, health or safety of any individual, or to public health or safety.

You must have a reasonable basis for your belief, and you must be able to justify it. The test is what a reasonable person, who is properly informed, would believe in the circumstances.

You cannot avoid obtaining consent just because it would be inconvenient, time-consuming or impose some cost. Whether these factors make it impracticable to obtain consent will depend on whether the burden is excessive in all the circumstances.

Example

A hospital is treating a seriously injured patient. The hospital asks you (the patient's usual GP) to disclose health information about the patient, which is needed to ensure the hospital can provide safe and effective treatment. Due to the nature and extent of his injuries, the patient is unable to consent to you disclosing the information. However, in this case you can disclose the information because it is reasonable for you to believe the disclosure is necessary to lessen a serious threat to the patient's life.

Conducting research, or the compilation or analysis of statistics

You may use or disclose a patient's health information if this is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety, and a number of other conditions are met. For further information, see Chapter 7.

Preventing a serious threat to the life, health or safety of a genetic relative

You can use or disclose a patient's genetic information without consent to prevent a serious threat to the life, health or safety of a genetic relative, provided a number of conditions are met. For more information, see Chapter 8.

Disclosure to a responsible person for an individual

Where a patient lacks capacity to consent, or is unable to communicate consent, you may be able to disclose health information to a responsible person for that patient. For more information, see Chapter 9.

For enforcement related activities

You can use or disclose health information where you reasonably believe that the use or disclosure is reasonably necessary for enforcement related activities conducted by, or on behalf of, an enforcement body. If you do so, you must make a written note of the use or disclosure.

Enforcement bodies include Commonwealth, State and Territory bodies that are responsible for policing, criminal investigations, and administering laws to protect public revenue or to impose penalties or sanctions. Enforcement related activities include the prevention, detection, investigation and prosecution or punishment of criminal offences, and intelligence gathering and monitoring activities.

You must have a reasonable basis for your belief that the disclosure is necessary, and you must be able to justify it. A disclosure is reasonably necessary if a reasonable person, who is properly informed, would agree that the disclosure was reasonable in the circumstances.

While the Privacy Act allows disclosure in this situation, it does not require disclosure. Other obligations, such as your duty of confidentiality, may affect whether you can disclose information to enforcement bodies.

Example: does the enforcement related activities exception apply?

A police officer was investigating a man's complaint that his neighbour had harassed him and damaged his property in an ongoing dispute. The officer phoned the man's GP to ask whether he 'was psychotic'. The GP disclosed that 'it was possible but further assessment was needed'.

Following this disclosure, the man made a privacy complaint to the Privacy Commissioner and the Commissioner made a determination on the matter.

The Commissioner concluded that, while the police force is an enforcement body, the GP could not rely on the 'enforcement related activities' exception and the disclosure therefore breached the Privacy Act. The Commissioner noted:

- there was no evidence that a warrant required the disclosure
- there was no suggestion that the officer's phone call related to an 'enforcement related activity'

- the GP had failed to consider the risks associated with disclosing the man's personal information without his consent, or that the GP had inquired about the purpose of the phone call to establish the severity of the situation.

Other situations

Other situations where you may use or disclose health information without consent include:

- to take appropriate action in relation to suspected unlawful activity or serious misconduct
- to locate a person reported as missing
- where reasonably necessary for establishing, exercising or defending a legal or equitable claim
- where reasonably necessary for a confidential alternative dispute resolution process.

For more information, see the Australian Privacy Principles (APP) Guidelines, Chapter C: Permitted general situations.

Overseas disclosure

Before you disclose health information to an overseas recipient, you must take reasonable steps to ensure that recipient does not breach the APPs in relation to that information. In addition, where you have disclosed health information to an overseas recipient, you will be accountable for any conduct the recipient engages in which would breach the APPs.

There are exceptions to these requirements. See the APP Guidelines, Chapter 8: APP 8 — Cross-border disclosure of personal information for more information.

Direct marketing

You can only use or disclose a patient's health information for direct marketing if the patient has provided consent. A patient's health information includes name and contact details.

Direct marketing is directly promoting goods or services to an individual, using personal information.

For more information, see Direct Marketing and Communications with patients.

Government related identifiers

You can only use or disclose a patient's government related identifier (such as the patient's Medicare number) in certain circumstances, including where the use or disclosure:

- is reasonably necessary for you to verify the patient's identity for your activities
- is reasonably necessary for you to fulfil your obligations to an agency or a State or Territory authority
- is required or authorised by or under an Australian law or a court/tribunal order

- in your reasonable belief, is reasonably necessary to lessen or prevent a serious threat to the life, health or safety of an individual, or to public health or safety
- in your reasonable belief, is reasonably necessary for enforcement related activities conducted by, or on behalf of, an enforcement body.

Healthcare identifiers are also regulated by the Healthcare Identifiers Act 2010.

See the APP Guidelines, Chapter 9: APP 9 — Adoption, use or disclosure of government related identifiers for more information.

Chapter 4: Giving access to health information

Contents

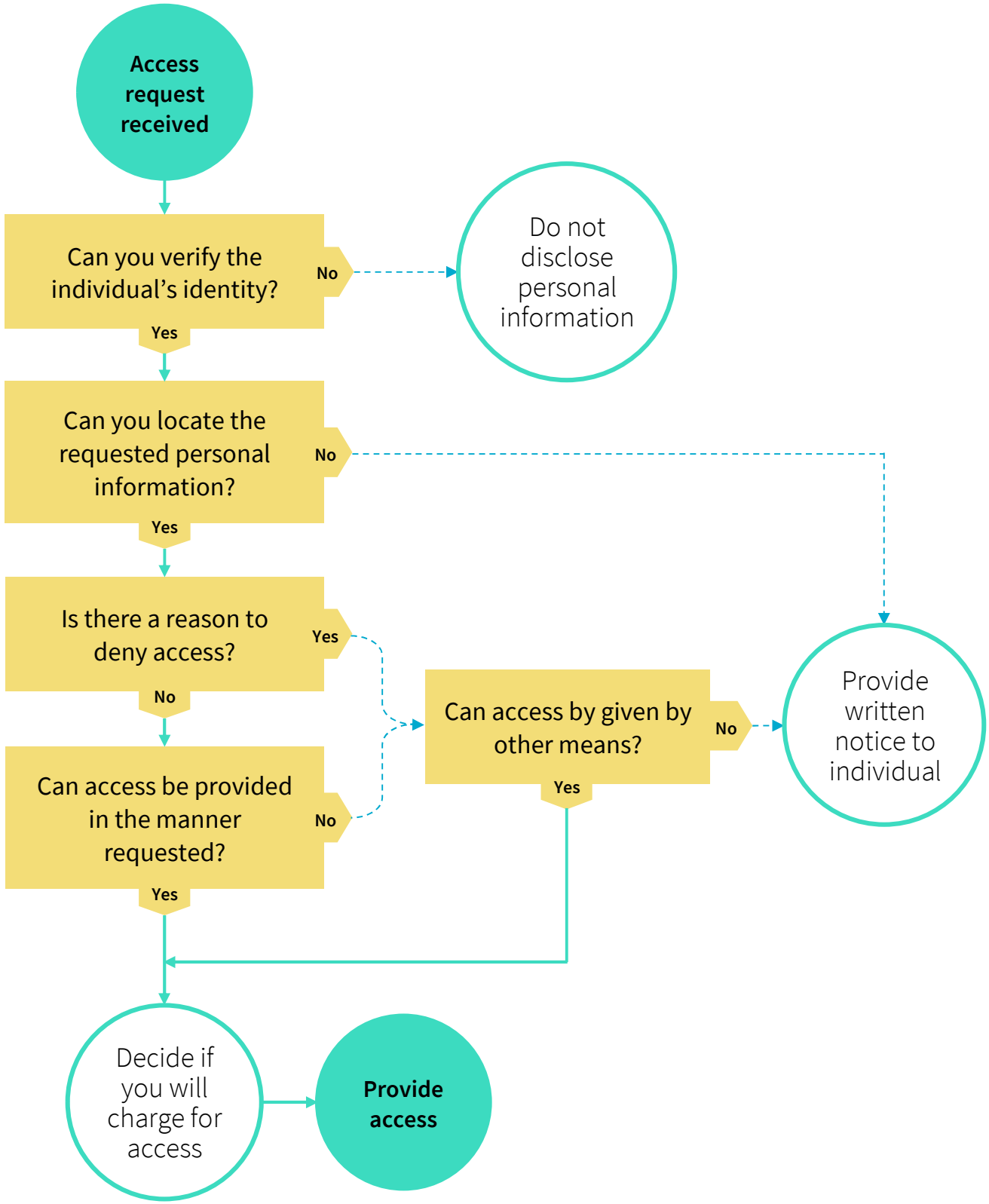
Key points 1
Overview of access requirements 2
Receiving a request for access 3
Verifying the patient's identity, or a third party's authorisation 3
Verifying the patient's identity 3
Access requests from a child's parent or legal guardian 3
Access requests from other representatives 4
Access requests from a third party organisation on a patient's behalf 4
Locate the requested health information in your records 5
Information received from other providers 5
Grounds for refusing access 5
Serious threat 6
Unreasonable impact on the privacy of other individuals 8
Giving access in the manner requested by the patient 8
Giving access by other means 9
Using an intermediary 9
Will you charge the patient? 10
Giving written notice 11

Key points

- Patients have a right to access information you hold about them, unless an exception applies.
- Generally, you must respond to a patient's access request within 30 calendar days.
- You must give access in the manner requested, unless it is unreasonable or impracticable.
- If you refuse to give access, or refuse to give access in the manner requested, you must:
  - take reasonable steps to give access in a way that meets both your own and the patient's needs
  - give the patient a written notice setting out the refusal grounds and complaint mechanisms.

Overview of access requirements

The flow chart below sets out the key steps to help you respond to a patient's access request. Further explanation of each step is included in the text following the chart.



Receiving a request for access

Patients' access requests can range from a request to access a single document or piece of information, to a request for a copy of an entire record. When responding to a request, you should try to give access in a manner that is as prompt, easy and as inexpensive as possible.

There are no formal requirements for a patient who is making an access request. You can ask a patient to follow a particular procedure (such as filling out a form), but you cannot require this (and in some cases a formal procedure is unnecessary, such as where a patient asks for a copy of pathology results during a consultation). However, developing a simple process may assist both you and your patients when dealing with access requests. Additionally, your privacy policy and privacy notice should set out how patients may access their health information.

You must respond to an access request within a reasonable period. In most cases, a reasonable period will not exceed 30 calendar days from when the patient makes the request.

Verifying the patient's identity, or a third party's authorisation

Verifying the patient's identity

You must ensure that the access request is made by the patient concerned, or by another person who is authorised to make the request on the patient's behalf (such as a legal guardian).

You should ask the patient for any evidence you may reasonably need to confirm identity. You should not disclose health information if you are not sure of the patient's identity.

What steps you need to take to verify identity depends on the circumstances. For example, if a regular patient requests access during a consultation, it is unnecessary to verify identity further. However, if you do not know the patient or have any doubt as to identity (for example, where access is requested via telephone), you should take steps to verify identity. It is preferable to simply sight identity documents, rather than make and retain copies.

Access requests from a child's parent or legal guardian

A child's parent or legal guardian might seek to access their child's records.

When considering such requests, you need to consider whether the parent is acting as a representative for the child, or whether the child has the capacity[1] to make the access request on his or her own behalf. If the child does have the capacity, then you should advise the parent or legal guardian that you believe the child has capacity and needs to make the request.

If the child does not have capacity, then you may be able to give access to the parent or legal guardian. However, you need to consider whether giving access to the particular representative is appropriate. You should consider who has care and responsibility for the child, whether there are court orders in place in relation to the care of the child, and whether a parent is unduly influencing

[1] For information about assessing a child's capacity, see Chapter 7.

a child. You should also consider whether the personal information of other individuals is contained within the records.

Access requests from other representatives

An adult patient who lacks capacity may need a representative (who has legal authority to act on the patient's behalf) to assist in accessing health information. Alternatively, a patient may simply authorise someone else, such as a partner, family member, carer or close friend, by providing a signed authority. If the representative is authorised to request access on the patient's behalf, you must give access (unless a refusal ground is available). However, you should first check the identity of the representative and verify that that individual has authority to act on the patient's behalf.

You should not give access if you are not satisfied the representative has proper authority. However, you could consider whether you can disclose the information under the use and disclosure provisions. For example, you may be permitted to disclose the information where the patient is unable to consent and where the disclosure is necessary for the patient's healthcare or for compassionate reasons.[2]

Access requests from a third party organisation on a patient's behalf

A patient may ask you to give a third party organisation access to health information, or you may receive a request for access to a patient's information from a third party (such as an insurance company or solicitor) on the patient's behalf, with the patient's consent.

If the patient asks you to give this information to a third party, you must do so unless there are grounds on which to refuse access.

If you receive the request from a third party, you must only give access to the information if you have the patient's consent. You must verify the patient's consent to ensure the access request is being made with the patient's authority. This includes considering:

- the nature and scope of the consent:
  - what exactly has the patient consented to?
  - does the scope of the third party's request match the patient's consent?
  - is the consent worded in a specific enough manner to allow you to understand what the patient has consented to?
- whether the consent is current: has the patient recently given consent, or is the third party relying on an undated or prior consent that may no longer reflect the patient's wishes?
- whether the patient has said or done anything to indicate consent may have been withdrawn, or that this consent may not have been given.

If you have any doubt about the validity of the consent, you should confirm the patient's understanding of what consent is being given. In addition, you should carefully consider what the third party is asking you to provide. If they are asking for documents relating to a particular condition, then you should only give access to those documents, not to a broader range of

[2] For more information, see Chapter 7.

documents or the patient's entire file. If it is unclear what you are being asked to provide, you could contact the third party to seek clarification.

If you give access when the patient's consent is not valid, or give access to documents other than those sought, it will be an unauthorised disclosure (unless the disclosure principles allow it).

Locate the requested health information in your records

You are required to give access to health information that you 'hold'.

You 'hold' health information if you have possession or control of a record that contains the health information. This includes information that a third party stores on your behalf but you retain the right to deal with the information.

When responding to an access request, you should search the records that you possess and control, including hard copy records and electronic databases including emails, calendars etc. You should also make enquiries of relevant staff or contractors.

Information received from other providers

Patients are entitled to access the health information you hold about them regardless of who authored particular documents, or who 'owns' the record. This means that, unless an exception applies, you must give a patient access to information you hold that you received from other health service providers, such as specialist reports.

Grounds for refusing access

The *Privacy Act 1988* (Privacy Act) contains ten grounds on which you can refuse to give access. These are:

- you reasonably believe that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety
- giving access would have an unreasonable impact on the privacy of other individuals
- the request for access is frivolous or vexatious
- the information relates to existing or anticipated legal proceedings between you and the patient, and would not be accessible by the process of discovery in those proceedings
- giving access would reveal your intentions in relation to negotiations with the patient in such a way as to prejudice those negotiations
- giving access would be unlawful
- denying access is required or authorised by or under an Australian law or a court/tribunal order
- you have reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to your functions or activities has been, is being or may be engaged in and giving access would be likely to prejudice the taking of appropriate action in relation to the matter

- giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body
- giving access would reveal evaluative information generated within your organisation in connection with a commercially sensitive decision-making process.

The two grounds most likely to arise for healthcare providers are discussed below. For information on the other grounds, see the Australian Privacy Principles (APP) Guidelines Chapter 12; refusing to give access.

If you decide not to give access based on one of the grounds listed above, you are required to take reasonable steps (if any) to give access in a way that meets your needs and the needs of the patient (see Giving access by other means below).

Serious threat

You can refuse to give a patient access to health information if you have reasonable grounds for believing it would pose a serious threat to the life, health or safety of the patient or another person, or to public health or safety.

Example: Refusing access due to serious threat

A psychiatrist treated a patient twice a week over a 10-year period for depression and severe bipolar. After her treatment with the psychiatrist ended, the patient made an access request to the psychiatrist seeking a copy of material that the psychiatrist had provided to the regulator in response to a complaint from the patient.[3]

The psychiatrist is concerned that giving access would cause significant distress to the patient and deterioration of her mental condition such that she would pose a threat to life, health and safety. This concern is based upon the psychiatrist's intimate knowledge of, and experience with, the patient's mental health condition, acquired during ten years of treatment.

While the patient has not sought treatment in a year, the patient has had the condition for several decades and, in the psychiatrist's opinion, it is lifelong and requires ongoing treatment. The illness has previously resulted in serious attempts on her life and multiple hospital admissions. The psychiatrist has observed that the patient's condition can become serious very quickly in response to trigger events.

Given these concerns and knowledge, the psychiatrist has a reasonable belief that giving access poses a serious threat to the patient. On this basis, the psychiatrist refuses to give access.

[3] This case study is adapted from a determination made by the Australian Privacy Commissioner in June 2017 ('LS' and 'LT' (Privacy) [2017] AICmr 60).

Helpful hint: assess the current risk

When considering serious threats, you must assess the risk at the time you are making the decision. On its own, the fact a patient has a history of serious mental illness is not a sufficient basis on which to refuse access. If you no longer treat the patient, or the patient has no recent threats of self-harm, it may not be reasonable to conclude that giving access poses a serious threat.

In the example above, while the psychiatrist was not currently treating the patient, it was reasonable to conclude that a serious threat existed at the time the access decision was being made. This was due to the length of the psychiatrist's treating relationship with the patient, and the knowledge and conclusions this allowed the psychiatrist to form about the patient's current state.

Helpful hint: be mindful of access rights when making clinical notes

When you make a clinical record of your interaction with a patient, you should be aware that, if the patient requests it, generally you would need to give the patient access to the notes. Being mindful of this possibility may influence the language you use and the approach you take to recording observations and clinical details. This may be a particularly relevant consideration in the areas of psychiatric and psychological care, but applies to all health service providers.

In some instances, an exception such as the serious threat exception may be genuinely available for you to rely upon to refuse access. However, feeling embarrassed or apprehensive about the patient reading your notes is not a legitimate ground for refusing access.

What if access would threaten the continuation of treatment?

If you believe that giving access would threaten your therapeutic relationship with the patient, and you have reasonable grounds for believing that the relationship breakdown itself would pose a serious threat to someone's life or health, you could deny access.

Example: Psychiatric care

A psychiatrist reasonably believes that a patient with severe mental illness would be so distressed if she saw the information in her record, that she would leave the psychiatrist's care and discontinue treatment altogether. The withdrawal from treatment could seriously threaten the patient's life, health or safety, and potentially that of her family. The psychiatrist could therefore refuse to give access.

However, the psychiatrist could not refuse access if he was only concerned that the patient may be unhappy with the information and might seek treatment elsewhere, or may discontinue treatment but the psychiatrist has no or little reason to believe that this may pose a serious threat.

Unreasonable impact on the privacy of other individuals

You should not give a patient access to health information if it contains another individual's personal information, and disclosing the information would have an unreasonable impact on that individual's privacy.

The following factors may be relevant in deciding whether the impact is unreasonable:

- the nature of the personal information – is it of a confidential nature?
- the other individual's reasonable expectations about how the personal information will be handled. For example, if both individuals were present when the information was collected, there may be a reasonable expectation that each individual could later access it
- the source of the personal information – for example, did the patient requesting access give you the information about the other individual when providing a family history.

If you plan to refuse access on this ground, you should:

- consider whether you can remove the personal information of the other individual so you can still give the patient access to the rest of the record (though you should take care to ensure the remaining context does not reveal the other person's identity)
- ask the other individual whether consent is given to some or all of the information being released. The individual's view may be relevant but not necessarily determinative. However, before consulting the individual, think about whether this in itself may impact on the privacy of the patient seeking access
- consider whether you can give access through an intermediary.

Giving access in the manner requested by the patient

Access to health information can be given in a variety of ways, such as:

- giving an electronic or hard copy of the information
- letting the patient view the information and take notes
- giving the information over the phone, such as test results
- giving the patient an accurate summary of the information
- allowing the patient to listen to or view the contents of an audio or video recording.

Where a patient requests access in a particular form, you must give access in the manner requested, unless it is unreasonable or impracticable for you to do so.

Whether a particular form of access is reasonable and practicable would depend on factors such as:

- the volume of information requested: for example, it may be impracticable to give a large amount of health information over the phone, but giving an electronic copy may be viable
- any special needs of the patient: for example, it may be reasonable to give information in a form that can be accessed via assistive technology where the patient has a vision impairment. You should also consider the level of understanding, language or literacy skills of the patient.

Helpful hint

For providers in NSW, Victoria or the ACT, local legislation may contain specific requirements relating to the form of access. For example, ACT and Victorian legislation gives patients express rights to request to have the information explained, and, when moving to a new provider, to ask their former provider to give their new provider a copy or written summary of their health record. Contact the Information and Privacy Commission NSW, Health Complaints Commissioner (Victoria) or ACT Health Services Commissioner to find out more about any additional requirements.

If a patient's preferred form of access is unreasonable or impracticable, you must consider other ways of giving access.

Giving access by other means

If you refuse to give access under one of the grounds listed above, or refuse to give access in the manner requested by the patient, you must take reasonable steps to give access in a way that meets your needs and the needs of the requesting patient.

You should talk to the patient to try to agree on a way to satisfy the request.

Some alternatives you could consider are:

- giving a summary of the information to the patient
- giving the patient the option of inspecting hard copy records and permitting the patient to take notes
- giving the information in an alternative format, such as electronically rather than physically
- facilitating access to the requested information through a mutually agreed intermediary
- blacking out any health information which you are entitled to refuse access to (such as information that unreasonably impacts on another individual's privacy) before giving access to the patient.

Using an intermediary

One option for giving access in another way is to use another health service provider as an intermediary. For example, giving a patient access to information through an intermediary might avoid a serious threat that you believe might arise if you give the patient direct access.

You should explain to the patient the role the intermediary will play, what information you will disclose to the intermediary and any costs involved. You and your patient should agree on the process and the intermediary to be used.

Example: considering alternative ways of giving access

After refusing to give access in the example above, the psychiatrist is now required to take reasonable steps (if any) in the circumstances to give access in an alternative way that meets both his own needs and the needs of the patient.

In some circumstances, there may be no reasonable steps that can be taken to meet both parties' needs. However, even if this is the conclusion, the psychiatrist must at least be able to demonstrate that he has considered whether any reasonable alternatives exist.

In this example, having considered alternative ways of giving access, the psychiatrist decides that the risk of the material posing a serious threat to the patient's life, health and safety can be managed by giving the patient access through a mutually agreed intermediary.

Helpful hint: intermediaries

Where you refuse access on the basis of the serious threat exception, you may be required under local legislation in NSW, Victoria or the ACT to give access through an intermediary if requested by a patient, or to allow an intermediary to consider whether access should be given. Contact your State or Territory regulator to find out more about any additional requirements.

Will you charge the patient?

You may charge a patient for giving access, provided the charge is not excessive in the circumstances.

Items for which you may charge include staff costs in searching for the requested health information, staff costs in reproducing and sending the health information, costs of postage or materials in giving access, and costs associated with using an intermediary to give access.

When charging fees for time and labour, patients should only be charged at a clerical rate for labour that clerical staff can perform (such as photocopying, printing, collating and posting documents). To the extent that professionals need to play a role, such as reviewing a file before giving access or creating a summary of clinical information, it may be reasonable to charge for time at their professional rate (or a proportion of it).

You could also consider offering cheaper ways of giving access if the patient prefers this, such as letting the patient view the information or giving an electronic copy.

The charge must not be excessive and you must not charge the patient for making the request. How much to charge, and whether a charge is excessive, needs to be considered in each case. This means that flat fees are generally not appropriate. In particular, in determining a charge, you need to consider characteristics of the requester, such as:

- your relationship with the patient
- known financial hardship factors affecting the patient
- known adverse consequences for the patient if access to the information is not gained.

A fee that may be appropriate for a patient who works full time may be excessive if imposed on a patient who receives a pension. In such cases, you should consider reducing or waiving any charge.

Whether a charge is excessive also depends on the nature of your practice, including its size, resources and functions, and the nature of the health information held.

Further examples of excessive charges include:

- a charge that exceeds the actual cost incurred by you in giving access
- a charge associated with getting legal or other advice in deciding how to respond to a request
- a charge for consulting with the patient about how access is to be given.

You must not impose a charge to discourage a patient from requesting access to their health information. You should clearly communicate and explain to the patient any charge you plan to impose, before access is given. You should invite the patient to discuss options for altering the request to minimise any charge. This may include options for giving access in another manner that meets both your and the patient's needs.

Example: imposing a charge

In the above example, the psychiatrist has incurred costs in giving the patient access. These costs include engaging another psychiatrist as an intermediary, and copying and sending the material to that psychiatrist.

The psychiatrist is aware that the patient has had difficulty maintaining employment due to her mental health condition, and receives a pension. Given the patient's personal circumstances, it would be excessive to charge the patient the full cost of giving access.

The psychiatrist therefore discusses with the patient options for altering the request to minimise costs. The patient decides she does not need access to the second opinion reports that were included in the material, and this alteration reduces the cost of copying and sending the material. While the psychiatrist still decides to impose a fee, the psychiatrist decides to waive the remaining copying and postage costs, and to share the cost of engaging the intermediary.

Helpful hint

Providers in Victoria and the ACT should be aware that the *Health Records Regulations 2012* (Vic) and *Health Records (Privacy and Access) Act 1997* (ACT) limit the charges that can be imposed for giving access and for transferring information to another health service provider. Contact your State or Territory regulator to find out more about any additional requirements.

Giving written notice

If you refuse to give access, or refuse to give access in the manner requested by the patient, and you cannot agree on an alternative form of access, you must give the patient a written notice setting out:

- the reasons why you have refused access, or refused to give access in the manner requested (except to the extent it would be unreasonable to do so)
- how the patient may make a complaint about your decision, how you will deal with the complaint and any information about external complaint avenues (such as the OAIC).

If you are refusing to give access in the manner requested by the patient, and you have not reached agreement on an alternative form of access, it can be useful for your written notice to set out the other ways in which you are willing to give access.

Example: Giving written notice

In the above example, if:

- the psychiatrist had continued to refuse to give access (having taken reasonable steps to consider alternative ways of giving access), or
- the patient had not agreed to receive access through an intermediary,

the psychiatrist would be required to give the patient a written notice.

The notice must set out the reasons why the psychiatrist is refusing access (except to the extent it would be unreasonable to do so), and how the patient can complain about the refusal (including how they can complain to the provider, and the subsequent external complaint options including to the OAIC).

In some instances, explaining the reason for refusal could be unreasonable, such as where even indicating that access poses a serious threat might in itself create a serious threat. However, in most situations, it would likely be possible to give some explanation of the reasons for refusal because the patient would normally have a general awareness of the content of the documents they are seeking to access, even if care needs to be taken in how that explanation is phrased.

Chapter 5: Correcting health information

Contents

Key points 1

When do you need to correct health information? 2

'Incorrect' information 2

Overlap with other privacy obligations 2

Correcting information on your own initiative 3

Dealing with a patient's correction request 3

Receiving a correction request 5

Verifying the patient's identity 5

Locating the patient's health information 5

Are you satisfied the information is incorrect? 5

Taking reasonable steps to correct the health information 5

Taking reasonable steps to notify another entity 6

Providing written notice 6

Associating a statement with the health information 7

Key points

- You must take reasonable steps to make sure the health information you hold is correct (given the purpose for which you hold it).
- This requirement applies where:
  - the patient requests that you correct the information
  - you otherwise become aware that health information you hold is incorrect.
- Generally, you must respond to a patient's correction request within 30 days.
- If you refuse to correct information, you must give notice to the individual.

When do you need to correct health information?

You must take reasonable steps to correct health information you hold about a patient if:

- you are satisfied the information is incorrect, or
- a patient asks you to correct the information.

'Incorrect' information

Health information is 'incorrect' if, given the purpose for which you hold it, it is:

- **Inaccurate:** Health information is inaccurate if it contains an error. An example is incorrect personal details held about a patient.

  Your medical opinion is not inaccurate just because a patient disagrees with it. Your opinion may be 'accurate' provided you present it as an opinion, it accurately records your view, and takes into account competing information and views.

- **Out-of-date:** Health information is out-of-date if it is no longer current.

  Health information may be out-of-date for some purposes but not others. For example, the fact your patient previously took a medication is out-of-date for the purposes of a current medications list. However, that same fact may not be out-of-date for the purposes of maintaining the patient's medical record in accordance with your professional obligations.

- **Incomplete:** Health information is incomplete if it presents a partial or misleading picture, rather than a true or full picture. For example, a physiotherapist's record for a patient seeking treatment for should pain is incomplete if it fails to note that the patient suffered a prior shoulder dislocation.

- **Irrelevant:** Health information is irrelevant if it does not have a bearing on or connection to the purpose for which it is held.

- **Misleading:** Health information is misleading if it conveys a meaning that is untrue or inaccurate.

Overlap with other privacy obligations

In addition to correction obligations, the *Privacy Act 1988* (Privacy Act) also requires you to take reasonable steps to ensure the quality of the health information you collect, use or disclose. 'Quality' of information refers to its accuracy, completeness, relevance, and whether it is current. Taking reasonable steps to ensure the quality of health information reduces the likelihood of information needing correction. Similarly, by taking reasonable steps to correct health information, you are helping to meet your obligations to ensure the quality of the health information you hold.

Helpful hint

An example of a step you can take to help ensure the quality of the information you hold is to periodically ask patients to confirm their details and emergency contact information.

Correcting information on your own initiative

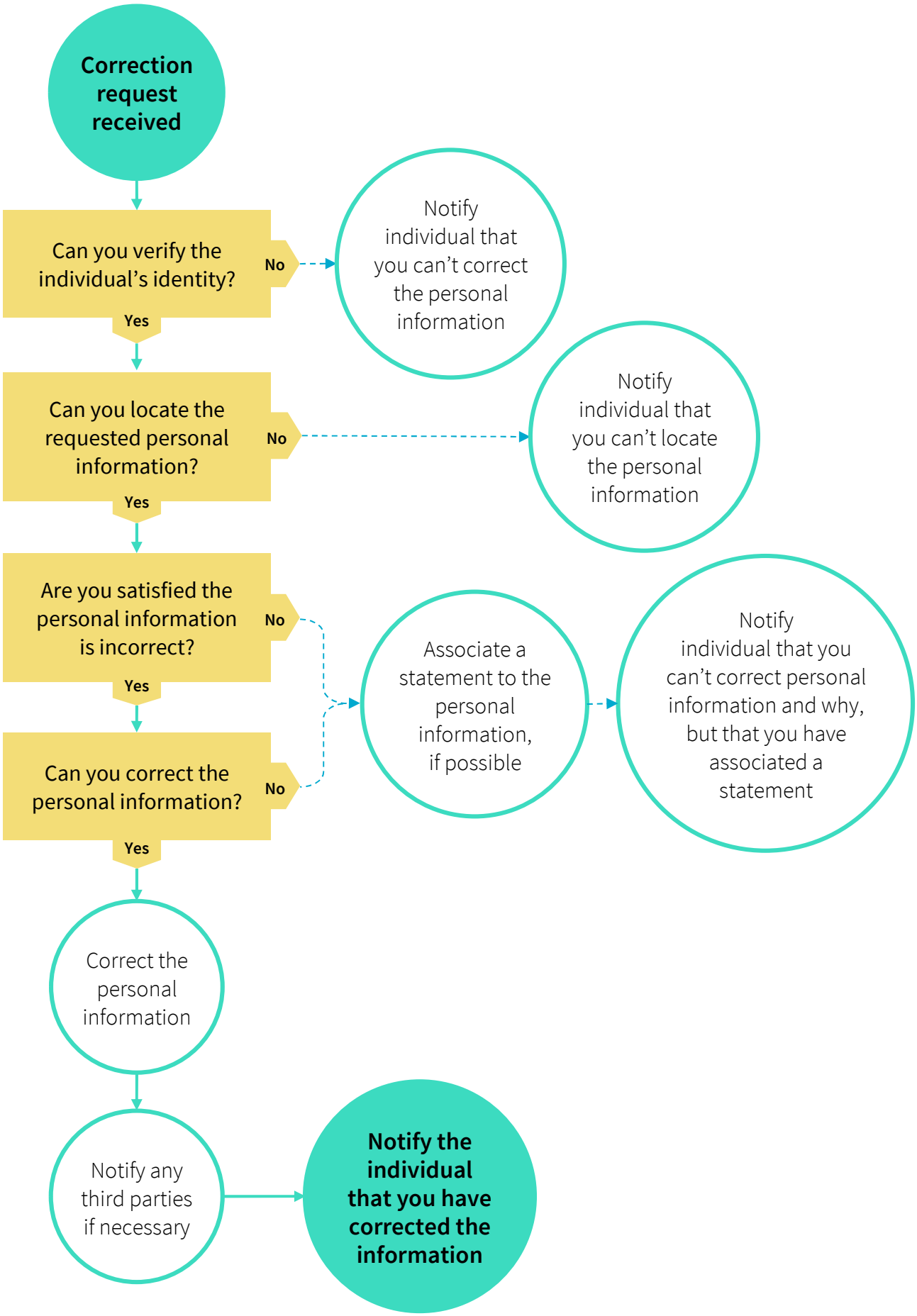
You are required to take reasonable steps to correct the health information you hold if you are satisfied that it is incorrect.

This requirement means that you should be alert to the possibility that health information you hold may be incorrect and require correction. Examples of when you may become aware that information you hold is incorrect include where you notice inconsistent information, where you are told by another party, and where practices, procedures or systems implemented in compliance with Australian Privacy Principle (APP) 1.2 that detect incorrect information.[1]

Dealing with a patient's correction request

The flow chart below sets out the key steps to help you respond to a request from a patient for correction of health information. Each step is explained further below the chart.

[1] For further information see the APP guidelines Chapter 1: APP 1 — Open and transparent management of personal information, 'Implementing practices, procedures and systems to ensure APP compliance'


Correction request received
Can you verify the individual's identity?
No
Notify individual that you can't correct the personal information
Yes
Can you locate the requested personal information?
No
Notify individual that you can't locate the personal information
Yes
Are you satisfied the personal information is incorrect?
No
Yes
Can you correct the personal information?
No
Associate a statement to the personal information, if possible
Notify individual that you can't correct personal information and why, but that you have associated a statement
Yes
Correct the personal information
Notify any third parties if necessary
Notify the individual that you have corrected the information

Receiving a correction request

A patient can ask you to correct health information you hold about them. Your privacy policy and privacy notice should set out how patients can make this request. While you can ask your patients to follow a particular process (such as filling out a form), you cannot require them to use that procedure.

You must respond to the patient's correction request (either by correcting the information or notifying the patient of your refusal to do so) within a reasonable period after the request is made. In most cases, a reasonable period will not exceed 30 calendar days.

You cannot charge a patient for making a correction request, for correcting the health information, or for associating a statement with the health information.

Verifying the patient's identity

You should ensure that a correction request is made by the patient concerned, or by another person who is authorised to make a request on the patient's behalf (such as a legal guardian).

In some cases, you may be confident of the patient's identity, such as where a regular patient asks you to correct information during a consultation. However, where it is less clear, you should ask the patient for any evidence you may reasonably need to confirm identity. It is preferable just to sight identity documents, rather than to make and retain copies.

If you are not sure of the requesting patient's identity, you should not correct the information.

Locating the patient's health information

Review your records to determine whether you hold the health information that needs correcting.

Are you satisfied the information is incorrect?

You must correct the health information if you are satisfied that, given the purpose for which you hold it, it is incorrect. You may ask the patient for further information or explanation if you are not satisfied that the health information is incorrect.

Taking reasonable steps to correct the health information

What are reasonable steps to take will depend on the circumstances. Reasonable steps include making appropriate additions, deletions or alterations to a record, or declining to correct health information if it would be unreasonable to take such steps.

Given the sensitivity of health information and the potential impact of it being incorrect, more rigorous steps are likely to be considered 'reasonable' than might be the case for other personal information.

Helpful hint

For practitioners in NSW, Victoria and the ACT, local legislation on correcting health information may contain more specific requirements. For example:

If you are a Victorian or ACT practitioner and consider that leaving incorrect information on a patient's record could result in harm, you may be required to place the incorrect information on a separate record. This record should not be generally available to other persons providing health services to the patient.

Victorian practitioners may be required under local legislation to record the name of the person who made a correction to health information, and the date it was made.

Where the deletion of incorrect health information is legally permitted, local legislation may require Victorian practitioners to make a written record of the name of the individual to whom the health information related, the period covered and the date the information was deleted.

Contact the Health Complaints Commissioner (Victoria), Information and Privacy Commission NSW, or the ACT Health Services Commissioner to find out about additional requirements.

Taking reasonable steps to notify another entity

If the patient asks you to, you must take reasonable steps to notify a third party[2] of corrections made to health information where you previously provided that information to that party. You are not required to do this if it would be impracticable or unlawful.

When you correct information, you should tell the patient you can be asked to notify third parties.

What are 'reasonable steps' depends on factors such as:

- the risk of adversity to the patient, for example if the information is clinically significant
- the nature of the correction, for example if the incorrect information is likely to impact on treatment by a third party
- the length of time since the information was disclosed, for example if the information is very old a third party may be less likely to rely on it
- the likelihood of it being used or disclosed again by a third party
- the practicability of notifying a particular third party.

Providing written notice

If you refuse to correct health information, you must give the patient written notice setting out:

- the reasons for your refusal (except where it would be unreasonable to do so)
- that the individual may request a statement be associated with the health information noting that the patient believes the information to be incorrect

[2] This applies to third parties covered by the Privacy Act (including all private sector health service providers and Australian government agencies). However, it would be best practice to inform other third parties.

- how the individual may make a complaint about your decision, how you will deal with the complaint and include information about external complaint avenues such as the OAIC.

If you do correct a patient's information, it would also be good practice to notify the patient of the correction and of the identity of any third parties you have notified about the change.

Associating a statement with the health information

If you refuse to correct health information, you should tell the patient that you can be asked to associate a statement with the information noting that the patient believes the health information to be incorrect.

If the patient asks you to associate a statement, you must take reasonable steps to associate it in a way that will make it apparent to other users of the health information. For electronic information, this may involve placing a flag on the information with a link to alert users where the statement is.

The content and length of any statement will depend on the circumstances, but generally, a statement would not be more than one page.

Chapter 6: Health management activities

Contents

Key points 1

'Health management activities' 1

Collecting for health management activities without consent 2

'Necessary' 2

De-identified information is not sufficient 2

Impracticable to obtain consent 2

Required by law, or in accordance with rules or guidelines 3

Reasonable steps to de-identify information before disclosure 3

Using and disclosing for health management activities 4

Key points

- Provided certain requirements are met, you can collect health information where it is necessary for health management activities.
- You can use or disclose health information for health management activities in accordance with the usual use and disclosure principles.

'Health management activities'

The *Privacy Act 1988* (Privacy Act) refers to 'the management, funding or monitoring of a health service' (referred to in this guide as 'health management activities').

'Health management activities' are likely to include activities that are reasonably necessary for the ordinary running of a health service. This includes activities that support the community's expectation that appropriately high standards of quality and safety will be maintained.

Examples of health management activities include where:

- a quality assurance body collects data about the quality of a nursing home health service
- an oversight body collects information from a private hospital about an incident that occurred during a patient's treatment
- a health insurer collects information relevant to possible fraud or an incorrect payment
- a health clinic reports to an accreditation body on the prevalence of patients who have had adverse drug reactions in the last two years.

Sometimes it is difficult to distinguish between a health management activity and a research activity. An activity is less likely to be research if its outcomes are limited in application to the

management, funding or monitoring of the specific entity undertaking the activity. If the activity produces an outcome that is more widely applicable to the health sector, then it may be research.

Collecting for health management activities without consent

While you normally need a patient's consent to collect health information, you can collect health information without consent where it is necessary for health management activities, and:

- the particular purpose cannot be served by collecting de-identified information
- it is impracticable to obtain the individual's consent, and
- the collection is either:
  - required by or under an Australian law (other than the Privacy Act)
  - in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation, or
  - in accordance with guidelines issued by the CEO of the National Health and Medical Research Council and approved by the Commissioner under s 95A of the Privacy Act.

'Necessary'

You may only collect health information that is 'necessary' for a health management activity. The term 'necessary' is applied objectively and in a practical sense. Collection is usually considered necessary if you cannot effectively carry out the health management activity without collecting the information. Collection is not necessary if it is merely helpful, desirable or convenient.

De-identified information is not sufficient

You must consider whether you can achieve the purpose of the health management activity by collecting de-identified information.

For example, to handle patient complaints effectively, you need to obtain patient contact details so that you can follow up and act on the complaint. In this case, you cannot effectively complete the health management activity with de-identified information.

Impracticable to obtain consent

Whether it is impracticable to obtain consent will depend on the circumstances. You will need to justify why it is impracticable to obtain a patient's consent. Incurring some expense or doing extra work does not in itself make it impracticable to obtain consent.

Examples of where it may be impracticable to seek consent include where:

- there are no current contact details for the individual and you have insufficient information to obtain up to date contact details
- obtaining the consent would adversely impact an investigation or monitoring activity.

Required by law, or in accordance with rules or guidelines

The collection must meet one of the following three criteria:

- required by or under an Australian law
- be in accordance with binding confidentiality rules established by competent health or medical bodies
- be in accordance with guidelines approved under s 95A.

Binding rules of confidentiality issued by competent health or medical bodies

The rules dealing with obligations of professional confidentiality must be binding on the organisation and have been established by a competent health or medical body.

Section 95A Guidelines

The National Health and Medical Research Council's *Guidelines approved under Section 95A of the Privacy Act 1988* (s 95A Guidelines) have been approved by the Information Commissioner and are legally binding. The s 95A Guidelines provide a framework for human research ethics committees to assess research proposals involving the handling of health information (without the consent of the subject). The framework requires ethics committees to weigh the public interest in research activities against the public interest in the protection of privacy.

Reasonable steps to de-identify information before disclosure

If you collect health information for health management activities without consent, you must take reasonable steps to de-identify that information before disclosing it.

Reasonable steps to de-identify information will depend on circumstances such as:

- the possible adverse consequences for an individual if the information is not de-identified before disclosure (and more rigorous steps are required as the risk of adversity increases)
- the practicability, including time and cost involved. However, you are not excused from taking particular steps to de-identify health information simply because it would be inconvenient, time-consuming or impose some cost. Whether these factors make it unreasonable to take a particular step will depend on whether the burden is excessive in all the circumstances.

Example

An incident monitoring body collects information, including health information, from a private hospital following the occurrence of a number of adverse incidents. The body collects this health information without the relevant patients' consent as it relied on the 'health management activities' exception (for the purposes of this example, it was impracticable to gain the patients' consent and using de-identified information was not possible).

As the information was collected under this exception, the body is required to take reasonable steps to de-identify the information before disclosing it. This means that, before issuing its report into the incidents, it must ensure that it takes reasonable steps to de-identify any patient health information that is included in the report.

Using and disclosing for health management activities

When using health information for a health management activity, you should always consider whether the proposed activity can be achieved using de-identified information.

If identified information is required, the normal use and disclosure provisions will apply.

Health information collected under the health management activities exception discussed above will have been collected for the primary purpose of a particular health management activity. You can therefore use and disclose the information for that purpose. However, as explained above, you must take reasonable steps to de-identify the information before disclosing it.

Where you originally collected the information you want to use or disclose for a health management activity for a different purpose, you will need to consider whether the use and disclosure provisions allow you to use or disclose it for health management activities. Relevant exceptions are:

- with patient consent
- use or disclosure that is reasonably expected and directly related to the primary purpose
- required or authorised by or under law.

Helpful hint

Use and disclosure principles in NSW, Victoria and the ACT health privacy legislation contain an express exception relating to health management activities. In some cases, additional requirements are contained in statutory guidelines, such as the NSW *Statutory guidelines on the management of health services*. For further information regarding these additional obligations, contact your State or Territory regulator.

Chapter 7: Disclosing information about patients with impaired capacity

Contents

Key points 1

Disclosure where the patient is unable to provide consent 1

Unable to give or communicate consent 2

Necessary for healthcare or compassionate grounds 3

Limiting disclosure to the extent reasonable and necessary for care or compassionate reasons 4

Ensuring disclosure is not contrary to expressed wishes 4

Key points

You can disclose a patient's health information to a 'responsible person' where:

- the patient lacks the capacity to consent or is unable to communicate consent, and
- the disclosure is either necessary to provide appropriate treatment, or is made for compassionate reasons.

Disclosure where the patient is unable to provide consent

While you can normally only use or disclose health information in accordance with the usual use and disclosure principles, you can disclose a patient's health information if all of the following conditions apply:

- you are providing a health service to the patient
- the patient is unable to give or communicate consent
- you only disclose the information to a responsible person for the patient
- the disclosure is either:
  - necessary for the provision of healthcare, or
  - made for compassionate reasons
- the disclosure is limited to the extent reasonable and necessary for the provision of care or treatment, or for compassionate reasons
- the disclosure is not contrary to the expressed wishes of the patient.

Unable to give or communicate consent

You can only disclose information in these circumstances where the patient:

- is physically or legally incapable of giving consent to the disclosure, or
- physically cannot communicate consent to the disclosure.

Incapacity

Patients may be physically or legally incapable of giving consent if they cannot understand the issues relating to the decision they are being asked to make, and are unable to form a reasoned judgement. This can occur on either a permanent basis (for example, when a patient has advanced dementia), or a temporary basis (for example, when a patient is unconscious).

Some patients may intermittently lose their capacity to give consent, or their capacity may gradually deteriorate because of illness. In such cases, you need to determine if the patient has sufficient capacity to indicate or withhold consent at the time of disclosure.

The following are examples of good practice:

- where a patient intermittently loses capacity, advise that you disclosed personal health information to the responsible person when the patient regains capacity
- where a patient gradually loses capacity, determine the patient's wishes for how health information is disclosed before capacity is lost.

Do children have the capacity to give consent?

The *Privacy Act 1988* (Privacy Act) does not specify an age after which individuals can make their own privacy decisions. As a general principle, a patient under the age of 18 has capacity to consent when the individual has sufficient understanding and maturity to understand what is being proposed.

Generally, you will need to assess each child's capacity to consent on a case-by-case basis. You will need to consider the child's maturity, degree of autonomy, understanding of the relevant issues and circumstances and the nature of the information being handled. Some young people in some circumstances will have sufficient competence to make their own decisions at a young age while some older teenagers may lack such competence. Other laws regarding obligations in relation to children or young people and their confidentiality may offer further guidance.

If you assess that a child lacks capacity to make personal privacy decisions, the child may still be able to contribute to decisions and should be involved in the decision making process to the extent possible.

Complexities arise in certain situations, such as:

- where a parent seeks health information about a child but the child explicitly asks that certain information not be disclosed. For instance, a child may reasonably seek health services in confidence, to address drug and alcohol, sexuality, suicide, depression and other mental illness or pregnancy issues. You may consider it appropriate, in the circumstances, to keep this information in confidence

- where there is parental separation or family breakdown it may be that only one parent or guardian has parental responsibility. In this case, you should clarify the arrangements when considering disclosing the child's health information
- in exceptional cases you may decide not to provide information about a very young child. This would generally be due to a risk of a serious threat to the child, or others, if you disclosed the information. For example, if a parent has a history of abuse, you may reasonably believe that disclosing the child's information would exacerbate that threat.

Unable to communicate consent

In some cases, a patient may be unable to communicate consent to the disclosure in any way (physically, verbally or in writing), even though the patient is able to develop an informed judgement. In this situation, you can disclose the health information to a responsible person (provided the other conditions outlined above are met). An example is a patient who has a physical condition or disease which impairs the ability to communicate, even though it does not impair capacity to consent.

Necessary for healthcare or compassionate grounds

You, as the individual practitioner providing the patient's healthcare, must be satisfied that either:

- the disclosure of information is 'necessary' to provide the patient with appropriate care or treatment, or
- the disclosure is made for compassionate reasons.

What is 'necessary' depends on the circumstances of each case. While the disclosure does not need to be critical for the provision of healthcare, it must be more than just a mere convenience. If a patient's care cannot continue or is diminished because you have not disclosed a particular piece of information, then disclosure would be considered necessary.

Example: disclosure necessary for healthcare

You are providing healthcare to a dementia patient. The patient has lost capacity and therefore is likely to forget to take her medication. Disclosing the patient's medication requirements to her carer therefore is necessary in order to ensure the patient receives appropriate care and treatment.

Example: disclosures for compassionate reasons

Examples of disclosures made for compassionate reasons may include:

- telling a patient's relative about the extent of the patient's injuries following a car accident
- where a cancer patient lacks capacity to consent, discussing his prognosis with a relative.

Limiting disclosure to the extent reasonable and necessary for care or compassionate reasons

When you are satisfied that disclosure is necessary for healthcare or that you are making the disclosure for compassionate reasons, you must limit the amount of information being disclosed to that which is reasonable and necessary for achieving that purpose.

In the example above where you disclose a patient's medication requirements, the extent of that disclosure must be limited to the information that is necessary and reasonable for providing healthcare. This means the disclosure would likely need to be limited to information about the prescribed medications, including drug names and dosages. It is unlikely to be necessary or reasonable to disclose information about previous unrelated medical procedures or diagnoses.

Ensuring disclosure is not contrary to expressed wishes

You must also ensure that the disclosure is not contrary to wishes expressed by the patient before becoming unable to give or communicate consent. This requirement applies to wishes of which you are aware, or of which you could reasonably be expected to be aware. These wishes may be recorded in the patient's file but do not have to be in writing.

Example

An aged care resident was admitted into a private hospital in an unconscious state following a fall. While treating her injuries, you discover in the aged care facility's notes for the patient that she has terminal bone cancer and has requested that this information not be disclosed to her family as she does not want to worry them. In these circumstances, disclosure of the bone cancer to the family may breach the Privacy Act.

Chapter 8: Using and disclosing genetic information in the case of a serious threat

Contents

Key points 1

Use or disclosure to lessen or prevent a serious threat 1

Lessening or preventing a serious threat 2

Section 95AA guidelines 2

Ensuring the accuracy of the genetic information 3

Collecting and using the contact details of a patient's genetic relatives 3

Ensuring the accuracy of the contact details 4

Key points

- Provided certain conditions are met, you can use or disclose a patient's genetic information to genetic relatives with or without the patient's consent where you reasonably believe the use or disclosure is necessary to lessen or prevent a serious threat to the life health or safety of a genetic relative of the patient.
- In a situation where consent has not been given the use or disclosure must also be in accordance with the s 95AA guidelines of the *Privacy Act 1988* (Privacy Act).
- The information in this Chapter is not intended to imply the existence of an obligation for health service providers to identify and contact all relatives who may be at high risk of having a genetic predisposition, but is aimed at clarifying how the Privacy Act applies to providers who choose to do so.

Use or disclosure to lessen or prevent a serious threat

A patient's genetic information can reveal information about inheritable diseases that may seriously threaten not just the patient's own health, but also the health of genetic relatives. With knowledge of their risk of a genetic condition, relatives may be able to take preventative or mitigating action.

In many cases, a patient who becomes aware of the risk of a genetic condition may choose to advise relatives personally, or may consent to you informing relatives.

While you normally need a patient's consent to use or disclose genetic information, you can use or disclose it without consent if you meet the following conditions (as set out in s 16B(4)):

- you collected the genetic information in the course of providing a **health service** to the patient
- you reasonably believe the use or disclosure is necessary to lessen or prevent a **serious threat** to the life, health or safety of a genetic relative of the patient
- you use or disclose the information in accordance with guidelines issued by the National Health and Medical Research Council and approved by the Information Commissioner under s 95AA of the Privacy Act (s 95AA guidelines)
- where you are disclosing the information, you disclose it to a genetic relative of the patient.

A genetic relative is an individual who is related to the patient by blood, such as a patient's sibling, parent or descendant.

You can also collect and use the personal information of the patient's genetic relative without the relative's consent, where it is unreasonable or impracticable to obtain their consent first, and you reasonably believe the collection and use is necessary to lessen or prevent a serious threat to the life, health or safety of that relative (Item 1 of the table at s 16A(1) *Privacy Act 1988* (Cth)). In practice, seeking prior consent from a relative in this scenario will usually be unreasonable or impracticable.

Lessening or preventing a serious threat

You can only use or disclose a patient's genetic information without consent if you reasonably believe that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of a genetic relative of the patient.

You must have a reasonable basis for your belief, and you must be able to justify it. The test is what a reasonable person, who is properly informed, would believe in the circumstances.

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 materialises. 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 (such as a genetic mutation that increases the risk of developing a certain cancer), may be a serious threat that can be lessened or prevented by disclosing the threat to the relative.

Section 95AA guidelines

If you are considering using or disclosing genetic information without the patient's consent, you must do so in accordance with the s 95AA guidelines. These legally binding guidelines are issued by the National Health and Medical Research Council and approved by the Australian Information Commissioner.

The guidelines require you to take reasonable steps to obtain the patient's consent for the use or disclosure of their genetic information before you proceed to use or disclose it without consent (see Guideline 3.2.3).

In addition, the guidelines outline the factors you should consider when determining if a use or disclosure of genetic information is necessary to lessen or prevent a serious threat to the life, health or safety of a patient's genetic relatives. They also provide guidance on matters such as good ethical practice, what to do when the patient or genetic relative is a child, contacting relatives, and the scope of information that is provided to relatives.

Ensuring the accuracy of the genetic information

Before using or disclosing a patient's genetic information, you should take reasonable steps to ensure that the genetic information is accurate, up-to-date, complete and relevant, having regard to the purpose of the use or disclosure. In some circumstances, it might be reasonable to take no steps, for example, where you have good reason to believe that the source of the information is reliable.

Example: Genetic testing of uncertain quality

A patient orders a 'direct-to-consumer' genetic test and brings the test results to you during a consultation. The report indicates that the patient may have haemochromatosis, a potentially serious heritable health condition. Relatives should be tested for the condition so that preventative measures can be taken. While the patient will inform his children, he does not consent to you disclosing this information to his siblings.

You are considering disclosing the information to the siblings, but you are concerned about the quality of the test. Referring the patient to a clinical genetics service for retesting in a laboratory with appropriate expertise might be a reasonable step to take to ensure the accuracy of the information before disclosing it.

Collecting and using the contact details of a patient's genetic relatives with or without consent

You can disclose a patient's genetic information to genetic relatives with or without the patient's consent, if a permitted situation exists, as outlined above. You will need to get the relatives' contact details from the patient, your own records, or from publicly available records.

The contact details of a genetic relative are 'health information' in these circumstances. While you would usually need the relative's consent to collect health information, you can collect the contact details without consent on the basis that it is unreasonable or impracticable to obtain consent, and you reasonably believe the collection is necessary to lessen or prevent a serious threat to the life, health or safety of that relative (Item 1 of the table at s 16A(1) *Privacy Act 1988* (Cth)). In practice, seeking prior consent from a relative in this scenario will usually be unreasonable or impracticable. Once you have collected the contact details, you can use them to contact the relative to inform them of their possible genetic risk, as this is the primary purpose for which you collected the information.

Alternatively, you may already hold a genetic relative's contact details in your records (for example, if that individual is your patient's 'next of kin' contact). You can use the genetic relative's contact details for the secondary purpose of informing that person of the potential risk of inheriting a genetic condition where you are satisfied that it is unreasonable or impracticable to obtain consent, and you reasonably believe the use is necessary to lessen or prevent a serious threat to the genetic relative's life or health (s 16B(4) of the Privacy Act).

It is likely to be impracticable to seek a relative's prior consent to collection or use of their contact details, as the health professional will not know about the relative other than through the patient and cannot contact the relative without collecting the contact details from the patient.

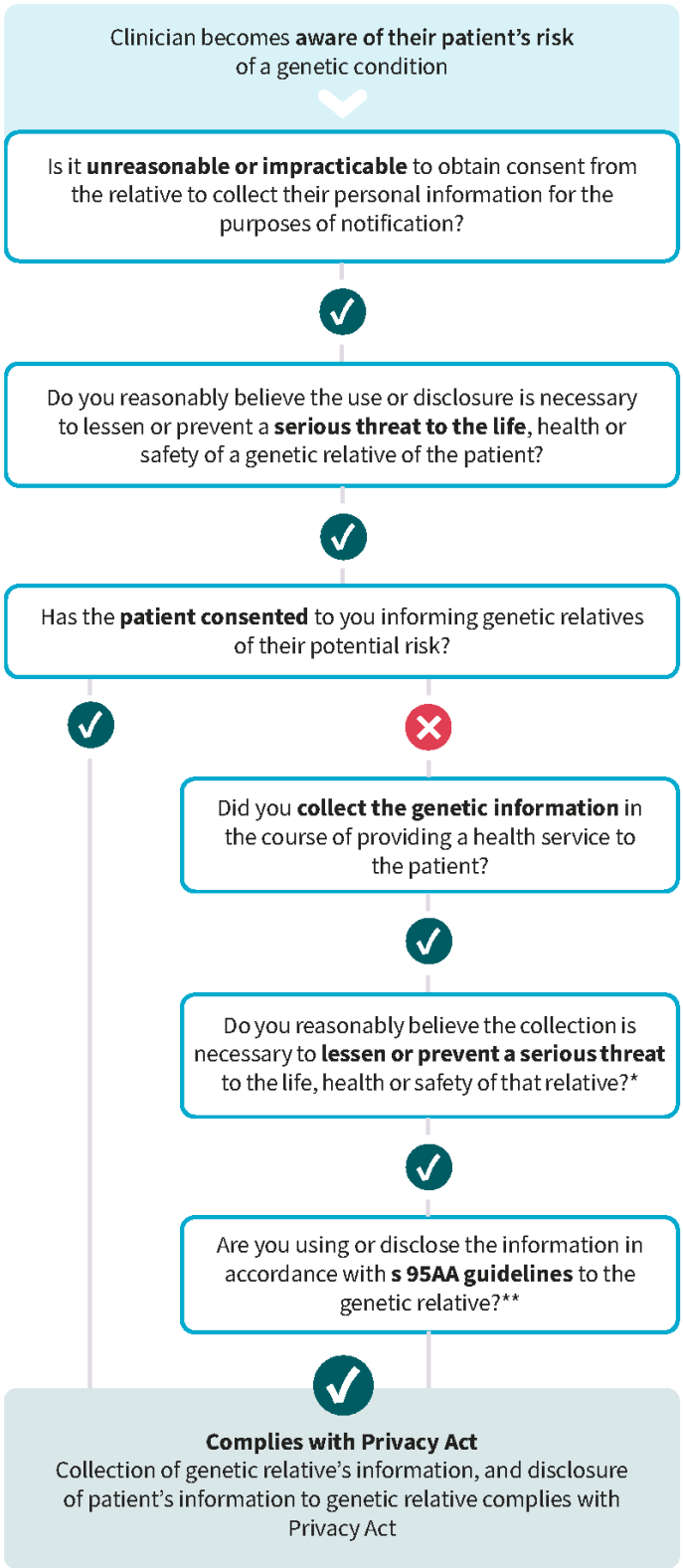
Example: Notifying at-risk relatives with consent of research participant

A patient participates in your research study and is found to have a genetic variant that confers a 50% risk of developing bowel cancer. The patient's genetic relatives are at risk of having inherited the same variant and should be notified of their potential risk and testing options. The patient advises they are not on speaking terms with their siblings but agrees they should be notified of their possible risk, and provides you with their postal and email addresses. In these circumstances, it is impracticable to seek the relatives' consent to collect or use their contact details. You can use the information to notify the relatives about their possible genetic risk and the opportunity to have genetic testing, if you believe doing so is necessary to lessen or prevent a serious threat to their life, health or safety.

Ensuring the accuracy of the contact details

Before collecting and using a relative's contact details, you should take reasonable steps to ensure that the contact details are accurate, up-to-date, complete and relevant.

Using contact details that are inaccurate, incomplete or out-of-date could have serious consequences for individuals. For example, the patient's genetic relative may remain unaware of the risk from an inheritable condition or, if you send the information to the wrong person, that person may be unnecessarily distressed.



* Item 1 of the table at s 16A(1) Privacy Act 1988 (Cth)
** 16B(4) Privacy Act 1988 (Cth)

Chapter 9: Research

Contents

Key points 1

Collecting health information for research without consent 1

- 'Necessary' 2
- 'Relevant to public health or public safety' 2
- De-identified information is not sufficient 2
- Impracticable to obtain consent 2
- Collection required by law, or in accordance with rules or guidelines 3
- Reasonable steps to de-identify the information before disclosure 3

Use or disclosure for research without consent 4

- 'Necessary' 4
- Reasonably believes the recipient will not disclose 4

Key points

Provided certain requirements are met:

- you can collect health information where it is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety
- you can use or disclose health information where it is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety.

Collecting health information for research without consent

While you normally need a patient's consent to collect health information, you can collect health information where it is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety, and:

- the particular research purpose cannot be served by collecting de-identified information
- it is impracticable to obtain the individual's consent, and
- the collection is either:
  - required by or under an Australian law (other than the *Privacy Act 1988*, (Privacy Act))
  - in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation, or

- in accordance with guidelines issued by the National Health and Medical Research Council and approved by the Information Commissioner under s 95A of the Privacy Act.

'Necessary'

You can only collect health information that is 'necessary' for the research or statistical exercise. The term 'necessary' is applied objectively and in a practical sense. Collection is usually considered necessary if you cannot effectively carry out the activity without collecting the information. Collection is not necessary if it is merely helpful, desirable or convenient.

'Relevant to public health or public safety'

To be relevant to public health or public safety, the outcome of the research or statistical exercise should impact on, or provide information about, public health or public safety.

Examples could include research and statistics on communicable diseases, cancer, heart disease, mental health, injury control, diabetes and the prevention of childhood diseases.

De-identified information is not sufficient

You must consider whether you can achieve the research or statistical aims by collecting de-identified information.

Example

A research project involves linking information about individuals from two or more electronic databases. You need identified information to correctly link the two data sets. In this case, de-identified health information will not achieve the project's purpose.

Helpful hint

When you hold health information, as a security measure you should de-identify information once you no longer need identified information. In the example above, you should de-identify the information once you have linked the two data sets and no longer require identified data.

Impracticable to obtain consent

Whether it is impracticable to obtain consent will depend on the circumstances. You will need to justify why it is impracticable to obtain a patient's consent. Incurring some expense or doing extra work does not in itself make it impracticable to obtain consent.

Examples of where it may be impracticable to seek consent could include where:

- there are no current contact details and there is insufficient information to get up-to-date contact details (this may occur in longitudinal studies involving old records)

- the integrity or validity of health research could be impaired, for example, because you are conducting a participant observation study and obtaining the consent of participants may alter their behaviour and the research results.

Helpful hint

Organisations arguing that consent is impracticable because it would invalidate the research methodology must have justifiable grounds for this view, including an independent opinion that does not come from researchers involved in the project. You could consider consulting a human research ethics committee about whether obtaining consent would have this effect.

Collection required by law, or in accordance with rules or guidelines

The collection must meet one of the following three criteria:

- be required by or under an Australian law
- be in accordance with binding confidentiality rules established by competent health or medical bodies or
- be in accordance with guidelines approved under s 95A.

Binding rules of confidentiality issued by competent health or medical bodies

The rules dealing with obligations of professional confidentiality must be binding on the organisation and a competent health or medical body must have established them. Generally, a binding rule is one that will attract a sanction or adverse consequence if breached.

Section 95A Guidelines

The National Health and Medical Research Council's *Guidelines approved under Section 95A of the Privacy Act 1988* (s 95A guidelines) have been approved by the Information Commissioner and are legally binding. The s 95A Guidelines provide a framework for human research ethics committees to assess research proposals involving the handling of health information (without the consent of the subject). The framework requires ethics committees to weigh the public interest in research activities against the public interest in the protection of privacy.

Reasonable steps to de-identify the information before disclosure

If you collect health information under this exception, you must take reasonable steps to de-identify that information before disclosing it.

What are reasonable steps to de-identify information will depend on circumstances such as:

- the possible adverse consequences for an individual if the information is not de-identified before disclosure (more rigorous steps will be required as the risk of adversity increases)
- the practicability, including time and cost involved. However, you are not excused from taking particular steps to de-identify health information simply because it would be inconvenient,

time-consuming or impose some cost. Whether these factors make it unreasonable to take a particular step depends on whether the burden is excessive in all the circumstances.

Use or disclosure for research without consent

You may use or disclose health information for research or statistical purposes relevant to public health or public safety when the Privacy Act permits the use or disclosure. For example:

- the individual has consented to the use or disclosure
- it is for the same (primary) purpose for which the information was collected
- it is for a purpose which is directly related to the primary purpose of collection, and the individual would reasonably expect you to use or disclose the information for that purpose.

However, you are also allowed to use or disclose health information where this is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety, and:

- it is impracticable to obtain the individual's consent
- the use or disclosure is conducted in accordance with the s 95A guidelines, and
- in the case of disclosure — you reasonably believe that the recipient will not disclose the information, or personal information derived from it.

Some of these concepts are outlined above. Two further concepts are discussed below.

Helpful hint

If you are conducting research in NSW, Victoria or the ACT, you may also be subject to additional requirements. While these requirements largely reflect the s 95A guidelines, some differences may exist. For instance, Victorian guidelines and ACT legislation refer to research, statistical compilation and analysis in the 'public interest' rather than research relating to 'public health or public safety'. Contact the Information and Privacy Commission NSW, Victorian Health Complaints Commissioner, or ACT Health Services Commissioner to find out more about any additional requirements.

'Necessary'

One aspect of considering whether a use or disclosure is 'necessary' is whether the particular purpose could be achieved by using or disclosing de-identified information. If so, the use or disclosure would not be considered necessary. De-identification is discussed above.

Reasonably believes the recipient will not disclose

Before disclosing health information using this exception, you must reasonably believe that the recipient will not disclose the information or personal information derived from it. You must have a reasonable basis for the belief, and must be able to justify it. The test is what a reasonable person, who is properly informed, could be expected to believe in the circumstances.

Helpful hint

You may have a reasonable belief that the recipient will not disclose the information if you have reviewed their research project plan and it does not involve the disclosure of the information. You could also seek written confirmation from the researcher that the information will not be disclosed.