

# 11 Using and disclosing personal health information (HPPs 10 and 11)

In general terms, a 'use' of personal health information refers to the communication or handling of information within NSW Health.

NSW Health is a single agency for the purposes of the Health Privacy Principles. Therefore, sharing health information between health services is considered a 'use' (see Section 3.2 NSW Health agencies to be treated as a single agency).

A 'disclosure' refers to the communication or transfer of information outside NSW Health. A disclosure can occur by:

- giving a copy of the information to another organisation or individual
- allowing another organisation or individual to access or view the information
- giving out summaries or communicating the information to another individual or entity in any other way.

As part of good clinical practice, patients should be included in decisions regarding the use and disclosure of their personal health information. This may occur, for example, at the time of collecting consent for treatment, or during consultation with the patient.

Use and disclosure are treated together as privacy law generally imposes the same conditions on both activities. An exception is that the disclosure provisions also allow disclosure on compassionate grounds (see Section 11.2.10), which does not apply to 'use'.

There are three broad categories of use and disclosure authorised under privacy law:

- where information is used or disclosed for the 'primary purpose' for which it is collected, OR
- where information is used or disclosed for another 'secondary purpose', and one of the criteria listed in the HPPs applies, OR
- where the use or disclosure of the information is lawfully authorised.

Activities which fall outside of these three categories are not permitted without patient consent unless a Public Interest Direction is obtained pursuant to section 62 of the [Health Records and Information Privacy Act 2002](#).

**NSW Health staff may only view, access, use and disclose personal health information when it is necessary for them to do so to carry out their work duties or for other authorised purposes.**

Section 15, Common privacy issues, provides guidance on how to address some common requests for use and disclosure of patient health information including requests for media access (see Section 15.7) and fundraising (see Section 15.8).

Staff must not access health information of family, friends or others for personal purposes unrelated to their work. If in doubt, staff should seek advice from a line manager and/or senior manager, local Health Information Service, or local Privacy Contact Officer.

## 11.1 Use and disclosure for the 'primary purpose'

A health service may use or disclose information it has collected for the purpose for which it was collected. The primary purpose will generally be the 'dominant purpose' for which the information was collected. Most often in the health system, the purpose for collecting personal health information will be to provide a health service.

### Examples

A person is admitted to hospital for exploratory surgery for suspected cancer. The 'primary purpose' for collecting their information at admission is to provide this service and will allow disclosure to those involved in the surgery, and others involved in providing the service, for example, health care providers including nursing staff, anaesthetists and pathologists.

Some months after the patient's discharge, the oncology unit proposes to conduct a fundraising drive, and proposes to use the information from health records to target recent admissions. As fundraising was not the 'primary purpose' for which this information was collected and is not an authorised secondary purpose under the privacy laws, the oncology unit can only use the personal health information for this purpose if patient consent for contact was obtained at the time of collection of their personal health information. Consent is required prior to using patient information for fundraising purposes.

## 11.2 Use and disclosure for a ‘secondary purpose’

The health service may also use or disclose information for another ‘secondary purpose’ if this is covered by one of the exemptions listed in HPPs 10(1) and 11(1). The secondary purposes listed under HPPs 10 and 11 are:

- use or disclosure for a directly related purpose, which would be ‘reasonably expected’ by the individual (see Section 11.2.1)
- use or disclosure to which the individual has consented (see Section 11.2.2)
- use or disclosure to prevent a serious threat to health or welfare (see Section 11.2.3)
- use or disclosure to assist in the stage of emergency (see Section 11.2.4)
- use or disclosure for management, training or research purposes (see Section 11.2.5)
- use or disclosure to assist in finding a missing person (see Section 11.2.6)
- use or disclosure as part of investigating and reporting wrong conduct (see Section 11.2.7)
- use or disclosure to or by a law enforcement agency or investigative agency (see Sections 11.2.8 and 11.2.9)
- disclosure made on compassionate grounds (see Section 11.2.10).

The information may also be used or disclosed if there is a ‘lawful authorisation’ to do so (see Section 11.3).

### 11.2.1 Directly related purpose HPP 10(1)(b) and 11(1)(b)

A health service may use or disclose the personal health information it has collected about an individual if it is a purpose which is **directly related** to the primary purpose, and the **individual would reasonably expect** the health service to use the information for this purpose.

All patients must be provided with the ‘Privacy Leaflet for Patients’. NSW Health staff should be aware that some patients will not share the same general expectations as other patients for a variety of reasons, for example, if they have previously received health care in a different country, or if they are particularly sensitive about aspects of their health care. Wherever practicable, NSW Health staff should make considered and respectful efforts as are reasonable in the circumstances to explain to patients how patient information is generally used and disclosed.

Sharing of health information for a directly related health care purpose often arises in the health system, particularly in relation to sharing information with other health care providers (see Section 15.1 Third party health care providers).

#### 11.2.1.1 ‘Directly related purpose’

This secondary purpose recognises there are activities that are necessary for health services to perform as part of their day-to-day operations, such as provision of ongoing care, billing and the following up of test results, which may not fall within the primary purpose for which the information was collected.

What is a directly related purpose will vary depending on the circumstances. There are however some common examples of what is likely to fall within the ‘directly related purpose’ exemption. These include:

#### Example

An antenatal unit from another hospital is requesting a copy of a patient’s health records relating to her previous pregnancy. As information relating to a previous pregnancy is likely to be relevant to the current pregnancy, it can be provided on the basis of ongoing care. It would also be expected that as a matter of good clinical practice the hospital requesting the information would have discussed this with the patient prior to making the request.

- using the information to provide ongoing care to patients
- disclosing health information to the patient’s nominated GP, other treating health services, hospitals or medical specialists involved in the care and treatment of a patient
- providing relevant health information to carers to assist with care for the patient
- using or disclosing NDIS documents, such as NDIS Plans, for the purposes of the [National Disability Insurance Scheme Act 2013](#), for example, to provide reasonable and necessary supports for NDIS participants, which may include sharing NDIS documents with third parties to help them provide reasonable and necessary supports for NDIS participants. If the information sought is unrelated to health care or is regarding financial entitlements, patient consent should be sought – see Section 4.1.11 NDIS. Contact your organisation’s Privacy Contact Officer for further information.
- sending reminders to a patient where the person receives a service on a regular basis or requires a follow up service

- administrative activities associated with providing, following up on or receiving payment for the service or product and follow up on an overdue payment (including disclosures to a debt collector). The information provided should be limited to what is relevant to the claim
- using the information to manage the provision of the service or product
- contacting a patient for feedback on the services received for the purpose of evaluation and improvement of services
- receiving and using patient information from approved remote patient monitoring platforms for the purpose of home monitoring
- providing relevant patient information to accredited hospital chaplains and pastoral care workers providing spiritual and pastoral care in accordance with the [Health Records and Information Privacy Regulation 2022](#) (see Section 11.2.11 Chaplaincy services)
- sharing relevant patient information with students and other staff for training purposes (see Section 11.2.5 and the [Statutory Guidelines](#))
- maintaining lists of patient names for patient care and safety purposes, for example, maintaining patient lists for fire evacuation for use by the fire brigade in event of an emergency
- using and disclosing patient information for purposes relating to the operation of the health service and treatment of patients, including funding, planning, safety and quality improvement activities
- using information for quality assurance or clinical audit activities carried out by the health service. This includes monitoring, evaluating or auditing the provision of the particular product or service which the health service has provided or is providing to patients (including activities undertaken to comply with the [NSW Patient Safety and Clinical Quality Program](#))
- disclosing information to an auditor or quality assessor for the purposes of monitoring, evaluating or auditing the provision of a particular product or service the health service has provided or is providing to the person (as long as the individual reviewing the health records is bound by privacy legislation or a professional code of ethics)
- some management and research activities may be considered a purpose directly related to health service delivery (see Section 11.2.5 Management, training or research)
- using and disclosing the information to investigate complaints about care provided by the health service or patient safety

- using and disclosing information to enable follow-up of complaints about the service or a product, or recalls of a product
- using or disclosing relevant information to claims managers and associated persons while managing a complaint, legal action or claim brought against the health service (See Section 12.5.4 Access by staff responding to a complaint, claim or investigation).

Staff with access to electronic health records may only access, view and use the system for authorised purposes. This means NSW Health staff may only view, access, use and disclose personal health information when it is necessary for them to do so to carry out their work duties, whether that be patient care or other directly related work duties that require access to personal and health information, for example, patient billing or human resource management. If in doubt about their obligations, staff should seek advice from a senior manager, local Health Information Manager or Privacy Contact Officer.

#### 11.2.1.2 'Reasonable expectation'

While the definition of directly related purpose is quite broad, the purpose must also be within the 'reasonable expectation' of the patient. This means that the purpose is closely related to the care and treatment **and/or** that the use or disclosure was communicated when the information was collected. The information given to the patient by the health service when the patient presents for care thus becomes important (the [Privacy Leaflet for Patients](#) and other information provided before or during clinical care).

Where it is made clear to the patient as part of the process of collecting their health information that their information may be used or disclosed for these purposes, then there is a more persuasive argument that the patient would 'reasonably expect' the health service to use or disclose their information in these ways.



#### Further guidance:

- Section 7 – Collecting personal health information (HPPS 1-4), sets out the types of information that needs to be provided and the ways it may be given.
- [Privacy Leaflet for Patients](#)

### 11.2.1.3 Outside a patient's 'reasonable expectation'

In rare circumstances, a patient may make a special request that their personal health information is not used or disclosed for purposes described in this Manual as directly related to the patient's health care (see Section 11.2.1.1 'Directly related purpose').

When health service staff receive such a request, the professional judgement of local health service staff will be required to resolve such requests on a case-by-case basis. To assist staff in exercising judgement, the following guidance is provided:

- A senior clinician should consider whether it is reasonable and practicable to meet the patient's request without putting the patient, staff member or any other person at risk of harm. Wherever it is possible to meet the patient's request, reasonable steps should be taken to comply with the request, and this should be documented in the patient's health record.
- Where it is not possible to comply with a patient's special request, a senior clinician (and other health service staff as necessary) should discuss with the patient:
  - a. the reasons for the patient's concerns about sharing the information
  - b. the reasons why there is a need to share information with all health service staff involved in their care
  - c. the obligations all staff have under privacy law to ensure all personal health information is kept confidential
  - d. the consequences for the patient's health care if personal health information is not shared. This conversation should also be documented in the patient's file.

If the patient remains of the view that they wish information to be withheld and it is the opinion of the treating health practitioner that sharing the information is essential to provide the health service in a safe or appropriate manner, the question then becomes one of whether the patient is prepared to consent to the treatment itself.

The service provider should explain this to the patient and that the facility is unable to provide health services to the patient given this effective refusal. Where appropriate, the facility may wish to offer to refer the patient to another facility or suggest that the patient considers seeking services from another facility.

It is anticipated that the occasions where a service provider will be required to consider the matter as a refusal of medical treatment will be extremely rare. Staff should work with the patient to resolve the issues and should also contact the Privacy Contact Officer for their health service to liaise with the patient and to participate in resolving such matters.

## 11.2.2 Consent

### HPP 10 and 11(1)(a)

This section is to be read in conjunction with Section 5.4 Consent.

#### 11.2.2.1 Where a third party seeks access

A patient can consent to or authorise any third party, such as a family member, interpreter, health practitioner (not involved in their ongoing care), legal representative, employer or insurer to have access to their health record.

Where health information is being used or disclosed on the basis of consent, consent must be provided by the patient prior to a third-party gaining access to a patient's health information.

Where the patient lacks the capacity to consent, the patient's authorised representative may consent on behalf of the patient (see Section 5.6 Authorised representative).

Where an immediate family member is unable to gain consent from the patient or the patient's authorised representative, for example, in circumstances of family dispute or estrangement, the health service may consider providing the family member with access to limited health information on compassionate grounds, see Section 11.2.10.

Where the patient is deceased, an immediate family member may be provided with access to relevant health records on compassionate grounds (see Section 11.2.10 Disclosure on compassionate grounds) or otherwise via a GIPA application. Additionally, an executor may be granted access to the deceased person's health records where they can demonstrate that the information is reasonably necessary to fulfil their legal duties.

Members of parliament making representations on behalf of a constituent are also required to have authorisation from the patient to make representations on their behalf.

#### 11.2.2.2 Procedures to follow to ensure the validity of the consent

The consent should be in writing and signed by the patient or their authorised representative.

A scanned copy, photocopy or photograph of the original consent document can be accepted when provided by the patient, third parties (such as the patient's legal representative or insurer) and other government agencies.

Where a patient's legal representative or insurer has electronic signing technology this may also be acceptable provided reasonable checks have been made to ensure the legal representative or insurer are verified.

The consent should contain:

- full name of patient
- date of birth
- contact details (current address, telephone number, email address)
- date of written consent (see Section 5.4.1 Elements of consent)
- details of the records or information sought, including range of dates for health treatment
- name of person being authorised and their relationship to the patient
- the purpose for which the information is requested (where relevant).

These requirements are to ensure both the patient and their health records are accurately identified, and to ensure only relevant information is released.

If the health service has reasonable grounds for concern regarding the validity or authenticity of the consent, it should contact the third party and/or patient directly for clarification.

The precise authority of the person requesting access and the nature of that access should be checked to ensure that only relevant material is released. Sometimes a health record will include information about people other than the patient. Health records should be carefully reviewed before release to check for and remove any third-party information in order to avoid a breach of privacy of the third party.

Where there are domestic and family violence concerns, care is needed to ensure the patient's consent is freely given and not pressured or coerced by the identified or suspected perpetrator or others acting on behalf of the perpetrator. Health workers should consult with a Senior Manager, Violence, Abuse, Neglect (VAN) Manager and/or VAN service representative as appropriate.



#### Further guidance:

- [Domestic Violence – Identifying and Responding \(PD2006\\_084\)](#)

Where the request is made for information related to an insurance or compensation claim, a scan or photocopy of the insurance application or compensation claim form signed and dated by the patient, containing the patient's consent to disclosure, is sufficient authority for the release of relevant health records. It will normally be sufficient for the health service to provide a medical report or summary of injuries for such claims to be processed. If further information is requested, only relevant sections of the patient's health record may be provided.



#### Further guidance:

- Section 12.6 Obtain proof of identity
- Section 15.6.3 Patient's Insurer

#### 11.2.2.4 Conditions of access

Access may be provided by direct access to the health information by provision of photocopies of relevant material, which is appropriately redacted, or viewing of the health record on the health service's premises. A health practitioner or health information manager (or other appropriately qualified personnel) must always supervise access to view original health records.

Confidential patient information must be transmitted securely. For further guidance, refer to information security measures set out in Section 9.2.4.

#### 11.2.2.5 Fees and charges

Where the person requests copies of a health record, the fees and charges may be required as set out in the relevant NSW Health policy and information bulletin.

The above requirements for consent and conditions of access also apply where the applicant is the patient's legal representative.



#### Further guidance:

- Section 5.4 Consent
- Section 12 Patient access and amendment (HPPs 6, 7 and 8)
- [Health Records and Medical/Clinical Reports – Charging Policy \(PD2006\\_050\)](#)
- [Health Records and Medical/Clinical Reports – Rates \(IB2019\\_036\)](#)

#### 11.2.2.6 Where the health service seeks to use or disclose

The proposed use or disclosure may also be initiated by the health service. This may be particularly relevant where the use or disclosure of the information is not a 'directly related purpose'. In such cases, the health service should:

- consider whether the patient has adequate capacity to give consent (see Section 5.4 Consent)
- address the elements of consent outlined in Section 5.4.1 Elements of consent
- make a written record of the consent, either through a written consent form signed by the patient, or by a contemporaneous note of a verbal consent recorded in the patient's health record.

In deciding whether to obtain a written or oral consent from the patient, the following factors should be considered:

- A written consent is the strongest evidence that the patient has given their consent. Written consent is required if there are many or complex issues the patient needs to consider before consenting. Consent would normally be obtained at admission, on commencement of the therapeutic relationship.
- Written consent should also be obtained where the information is proposed to be used or disclosed for a purpose unrelated to the reason for its collection, for example, using a 'good news' story in a hospital newsletter, or for fundraising (see Section 15.8 Fundraising).
- Written consent is not required for day-to-day disclosures relating to ongoing care and treatment, or actions covered by an existing written consent, or where it is otherwise allowed under the Health Privacy Principles.

### 11.2.3 Uses and disclosures regarding threats to health and safety, and public health HPP 10 and 11(1)(c)

A health service may use or disclose personal health information if there are reasonable grounds for believing that this is necessary to lessen or prevent:

- a **serious and imminent threat** to the life, health or safety of the individual or another person, or
- a serious threat to **public health or public safety**.

#### 11.2.3.1 General guidelines

Health staff should be aware that these situations are unlikely to arise in day-to-day case management and so disclosure on this basis will be a relatively uncommon occurrence.

In circumstances where a health practitioner considers that a patient represents a risk to themselves or others, they should carefully assess the level of risk before acting. It is advisable to discuss the situation with an appropriate manager, senior health practitioner or colleague before acting (as is practical and time permitting).



#### Further guidance:

- [Domestic Violence – Identifying and Responding \(PD2006\\_084\)](#)

### Examples

A patient of a community health service arrives in an agitated state, making threats against a close family member over a custody dispute. The patient has a history of violence and faced previous assault charges over the same matter. Staff would have reasonable grounds to believe the relative was at serious risk, and so could disclose the information to address this risk.

A Public Health Unit which is investigating and monitoring confirmed or suspected cases of meningococcal infection on a cruise ship which has now left NSW but will be stopping at another Australian port shortly. The Unit would be entitled to share the information with relevant authorities to ensure the serious public health risk is properly addressed as soon as possible.

#### 11.2.3.2 Where staff may be at risk

Sharing of information about a patient's violent behaviour is permitted when the patient is referred or transferred within or between facilities (including community health services, aged care facilities and other similar facilities), and when the patient poses a threat to themselves or any individual including staff, or to public health or public safety. Key principles for managing violent behaviour are:

- Privacy obligations must be balanced with health service's obligations to ensure a safe workplace under the [Work Health and Safety Act 2011](#).
- Relevant patient information should be made available when referring or transferring a patient to ensure patient and staff safety during transfer and to prevent adverse incidents.
- When sharing information about a patient, focus on patient behaviours that may pose a threat or risk, and appropriate patient management strategies.
- A health service must take reasonable steps to ensure the information they share is relevant, accurate, up to date, complete and not misleading.
- Use patient alerts or patient flagging in accordance with '[Preventing and Managing Violence in NSW Health Workplace – a Zero Tolerance Approach](#)'.



#### Further guidance:

- [Preventing and Managing Violence in NSW Health Workplace – a Zero Tolerance Approach' \(PD2015\\_001\)](#)
- [Violence Prevention and Management Training Framework for NSW Health Organisations \(PD2017\\_043\)](#)

**Contact:** [Workplace Relations Branch, NSW Ministry of Health](#)

### 11.2.3.3 Public Health Act 2010 – Public health risks and public health orders

The [Public Health Act 2010](#) allows for the disclosure of personal health information in limited circumstances between authorities and practitioners where it is suspected on reasonable grounds that a person has a category 4 or 5 condition and the failure to provide the information could place the health of the public at risk. A category 4 or 5 condition includes HIV and TB.

If staff are concerned about a possible health risk relating to HIV or the behaviour of an HIV positive person, they should contact their local HIV coordinator, or the [Centre for Population Health](#), NSW Ministry of Health.



#### Further guidance:

- [Management of people with HIV who risk infecting others \(PD2019\\_004\)](#)

### 11.2.3.4 Public Health Act 2010 limitations on disclosure of information indicating a person's HIV status

Section 56 of the [Public Health Act 2010](#) provides that a person who, in the course of providing a service, including the conduct of a pathology test, acquires information that another person:

- (a) has been, is to be or is required to be tested for HIV, or
- (b) has, or has had, HIV or AIDS,

must take all reasonable steps to prevent that information from being disclosed to any other person.

Section 56 of the [Public Health Act 2010](#) places strict limitations on the release of this information. This information can only be disclosed:

- with the consent of the person concerned, or
- to a person who is involved in the provision of care, treatment or counselling to the person concerned, or
- to the Secretary, if a person has reasonable grounds to suspect that failure to disclose the information would be likely to be a risk to public health, or
- in connection with the administration of the [Public Health Act](#) or the regulations, or
- for the purposes of any legal proceedings arising out of the [Public Health Act](#) or the regulations, or of any report of any such proceedings, or
- in accordance with a requirement imposed under the [Ombudsman Act 1974](#),
- in accordance with the [Mandatory Disease Testing Act 2021](#); or
- in the circumstances prescribed by the regulations.

Information relating to a person's HIV status can be made available to clinical staff if it is relevant to the patient's care for any health condition.

However, health services need to be aware that the requirement to appropriately manage HIV information is still higher than for other types of health information. Most significantly, the exceptions that allow for use and disclosure of other types of health information for secondary purposes, such as research, training, and management, do not apply to HIV information. Staff need to understand that any release or discussion of the HIV information that is not subject to the exemptions could be an unlawful disclosure in breach of the [Public Health Act 2010](#).

The Act provides for a penalty of up to 100 penalty units (\$11,000) or imprisonment for 6 months, or both, for a breach of section 56 without reasonable excuse.



#### Further guidance:

- Section 15.9.6 Managing public health risks
- [Management of People with HIV Who Risk Infecting Others \(PD2019\\_004\)](#)
- [Tuberculosis Management of People Knowingly Placing Others at Risk of Infection \(PD2015\\_012\)](#)
- [Management of health care workers with a blood borne virus and those doing exposure prone procedures \(PD2019\\_026\)](#)
- [Disclosure of Unit Record Data for Research or Management of Health Services \(PD2015\\_037\)](#)
- Section 15.14 – NSW data collections

### 11.2.3.5 Genetic information

The [Health Records and Information Privacy Act 2002](#) allows for the disclosure of genetic information to genetic relatives without patient consent, albeit in very limited circumstances. Genetic relative means a person who is related to an individual by blood, for example, a sibling, parent or descendant of the individual.

Under HPPs 10 and 11(1) (c1) genetic information can be used and disclosed where:

- The disclosure is to a genetic relative of the individual to whom the genetic information relates, and
- It is reasonably believed to be necessary to lessen or prevent a serious threat to the life, health or safety (whether or not the threat is imminent) of that genetic relative, and
- The disclosure is made in accordance with guidelines, if any, issued by the NSW Privacy Commissioner.



### Further guidance:

- The NSW Information and Privacy Commission [Use and disclosure of genetic information to a patient's genetic relatives: Guidelines for organisations in NSW](#)

The Guidelines encourage health practitioners to take all reasonable steps to obtain consent from the patient (or the patient's authorised representative), and to consult with other experienced health practitioners in the first instance. They also make clear that if a disclosure occurs, only information that is necessary to communicate the risk of harm should be disclosed and, where possible, the patient should not be identified.

The Guidelines may assist an individual and their health practitioner to gain access to relevant records of a deceased genetic relative of the individual where the individual is considered to be at serious risk. Alternatively, where the deceased person is 'an immediate family member', the genetic relative may wish to seek access to the health records on compassionate grounds (see Section 11.2.10 Disclosure on compassionate grounds).

It should be noted that the scope of the Guidelines does not include situations where genetic information presents a serious threat to an unborn child. The patient's consent to disclose genetic information about themselves to a pregnant mother would be required.



### Further guidance:

- Section 11.2.10 Disclosure on compassionate grounds

## 11.2.4 To assist in a 'stage of emergency'

Exemptions apply to handling of personal information in a 'stage of emergency' as defined in the [State Emergency and Rescue Management Act 1989](#) (HPP 10 and 11(1)(b1)).

An 'emergency' is defined as an emergency due to actual or imminent occurrence (such as fire, flood, storm, earthquake, explosion, terrorist act, accident, epidemic or warlike action) which

- endangers, or threatens to endanger, the safety or health of persons or animals in the State, or
- destroys or damages, or threatens to destroy or damage, property in the State, or
- causes a failure of, or a significant disruption to, an essential service or infrastructure, being an emergency, which requires a significant and co-ordinated response.

A health service may use or disclose personal health information to assist in a 'stage of an emergency', where the use or disclosure of the information is reasonably necessary to assist in the stage of the emergency, and it is impracticable or unreasonable for the organisation to seek the consent of the individual to whom the information relates.

For the purposes of considering whether a situation amounts to a stage of emergency. Consider the 4 stages of an emergency set out in the [State Emergency and Rescue Management Act 1989](#):

- **prevention** in relation to an emergency includes the identification of hazards, the assessment of threats to life and property and the taking of measures to reduce potential loss to life or property, and
- **preparation** in relation to an emergency includes arrangements or plans to deal with an emergency or the effects of an emergency, and
- **response** in relation to an emergency includes the process of combating an emergency and of providing immediate relief for persons affected by an emergency, and
- **recovery** in relation to an emergency includes the process of returning an affected community to its proper level of functioning after an emergency.

For example, a hospital or district may consider releasing the names and addresses of all home dialysis patients in a fire risk area to Police or Fire and Rescue NSW when a fire or flood is threatening to endanger those patients. This enables appropriate assistance to be provided to these patients to manage any evacuations and ongoing dialysis in the event of a power outage.

However, under this exemption, if a NSW Health organisation (or another public sector agency) collects, uses or discloses personal information relying on the stage of emergency exemption, it must not hold the information for longer than 18 months, unless extenuating circumstances apply, or consent has been obtained.

This means that the address lists and patient details (described above) provided to Fire and Rescue NSW or Police and prepared by Hospitals or Districts for the sole purpose of the stage of emergency are not to be held for longer than 18-months (after the date of collection). Unless consent is obtained or in extenuating circumstances.



### Further guidance:

- 11.2.8.5 Law enforcement requests in emergency circumstances

## 11.2.5 Management, training or research HPPs 10 and 11 (1) (d), (e) and (f)

A health service may use or disclose personal health information:

- if it is reasonably necessary for:
  - **funding, management, planning or evaluation** of health services; or
  - **training** the health service’s staff members or people who work with the health service; or
  - **research** or the compilation or analysis of statistics in the public interest; AND
- the use or disclosure is in accordance with [Statutory Guidelines](#) issued by the NSW Privacy Commissioner.

### 11.2.5.1 When to use this exemption

Many funding, management, and planning purposes will be a ‘directly related purpose’ (see Section 11.2.1.1), so you should first check if that exemption applies before considering these exemptions.

For example, data matching of patient information by a health service may be ‘directly related’ to care if it is required to plan and manage patient care requirements and to ensure staffing, surgery access, bed availability and other management needs are met.

Each of the exemptions for management, training and research has certain preconditions before it can be applied. These are:

#### **The use or disclosure is reasonably necessary for the purpose**

The health service must consider to what degree the personal health information is needed for the activity. For example, sometimes the activity may be just as effectively undertaken using hypothetical case studies, or simulated situations.

#### **The purpose cannot be served by de-identified information**

If the activity could be undertaken by using/ disclosing de-identified information, the provision requires the health service to proceed in that way. This may involve converting ‘identifiable’ information (information that allows identification of a specific individual) into ‘de-identified’ information.

De-identified information is information from which identifiers have been permanently removed, or where identifiers have never been included.

Sometimes de-identified information cannot achieve the purpose of the management of health services activity. This could be, for example, where an activity involves linking information about individuals from two or more sources and identified information is needed to correctly link records from each data source.

### **It is impracticable to seek the person’s consent**

The fact that seeking consent is inconvenient or would involve some effort or expense is not of itself sufficient to warrant it to be considered ‘impracticable’. Some examples of where it might be impracticable to seek consent include if:

- the age or volume of the information is such that it would be very difficult or even impossible to track down all the individuals involved
- there are no current contact details for the individuals in question and there is insufficient information to get up-to-date contact details
- a complete sample is essential to the integrity and success of the management of health services activity and the activity would not be possible if any persons refused to allow their information to be used.

### **Reasonable steps have been taken to de-identify the information**

When de-identifying information, you should consider the capacity of the person or organisation receiving the information to re-identify it or link it to identifiable information.

Removing the name and address may not always be enough, particularly if there are unusual features in the case, a small population, or there is a discussion of a rare clinical condition.

Reasonable steps to de-identify might also include removing other features, such as date of birth, ethnic background, and diagnosis that could otherwise allow an individual to be identified in certain circumstances.

Controls and safeguards in the data access environment should be put in place to minimise the risk of re-identification.

### **The information will not be published in a generally available publication**

A ‘generally available publication’ is a publication that is generally available to members of the public, either in paper or electronic form.



#### **Further guidance:**

- IPC [Statutory Guidelines](#)
- [De-Identification Decision-Making Framework](#), OAIC and the CSIRO.
- [Fact Sheet: de-identification of personal information, Information and Privacy Commission \(IPC\)](#)
- [Privacy issues and the reporting of small numbers](#), HealthStats NSW
- [Disclosure of unit record data by Local Health Districts for research or contractor services \(PD2018\\_001\)](#)

### 11.2.5.2 Statutory guidelines

The NSW Privacy Commissioner, Information and Privacy Commission NSW, has issued [Statutory Guidelines](#) that set out conditions imposed on use and disclosure of personal health information for management, research and training.

To view the relevant [Statutory Guidelines](#) go to:

- [Management of health services](#)
- [Training](#)
- [Research](#)

#### Management guidelines

The management guidelines discuss each of the preconditions in detail and draw attention to the relevant 'directly related purpose' which may otherwise apply.

In circumstances where the activities may go beyond a routine management of health services activity and do not appear to come within the 'directly related purpose' exemption, the guidelines provide some further threshold questions to consider before a proposal for the activity must be approved by a Human Research Ethics Committee.

A Human Research Ethics Committee will consider the proposed use or disclosure and assess whether, on balance, it is in the public interest prior to the organisation using or disclosing health information for the purpose of the activity.

#### Research guidelines

The research guidelines are consistent with and mirror the guidelines developed by the NHMRC under sections 95 and 95A of the [Privacy Act 1988](#) (Cth). Research requiring use or disclosure of personal health information will need to be considered by a Human Research Ethics Committee.

#### Training guidelines

The training guidelines define the circumstances in which personal information can be used in training. The emphasis is on de-identifying the information, except in cases such as student placements and certain staff training where de-identification would defeat the purpose of the training. The guidelines then set requirements for managing such training and the obligations on health services to appropriately protect the information if it is identifiable.

Health organisations seeking to use or disclose health information relying on the 'training exemption' in Health Privacy Principle 10(1)(e) or 11(1)(e) must:

- (a) be reasonably satisfied that the training will make those being trained aware of the privilege that they are being granted; and

- (b) take reasonable steps to ensure that any notes (or other forms of record) containing identifying data and made by persons accessing the information are kept to a minimum.

The guidelines recognise a distinction between training and demonstrations and education programs involving clinical placements as follows:

#### Training and demonstrations

The anonymity of patients should be maintained during case presentations, demonstrations, research activities and at seminars and conferences. Where possible, fictitious data should be used.

Use of photos, slides and other visual aids which allow identification of individuals should not occur unless the material is of critical importance and the consent of the patient has been obtained.

Individual features which may identify individuals include their face, birth marks, scars, tattoos, piercings, and other features which may be unique to an individual.

A cultural sensitivity warning may be required for Aboriginal and Torres Strait Islander students when clinical records identifying a deceased indigenous person are used for education or training purposes.

#### Clinical placements and students

Students may have access to health records with the approval and under the direction of their supervisor if that access is sought in respect of their education program at the health facility. Access does not include photocopying or transcribing records containing personal health information or taking such health records off-site. Patients may refuse to have a student participate in their treatment.

Student health professionals must sign a [NSW Health privacy undertaking](#) and must comply with privacy law and all NSW Health policies.



#### Further guidance:

- NSW Privacy Commissioner [Statutory Guidelines on Training](#)
- Section 9.2.6 Training and presentations
- [Disclosure of Unit Record Data for Research or Management of Health Services \(PD2015\\_037\)](#)
- See clinical documentation responsibilities for students in: [Health Care Records – Documentation and Management \(PD2012\\_069\)](#)

## 11.2.6 Finding a missing person

### HPPs 10(1)(g) and 11(1)(h)

A health service may use or disclose personal health information if the information is to be used by a law enforcement agency to ascertain the whereabouts of a missing person. This exemption only applies if the person has been reported to the police as missing.

#### Example

Police have received a report from a family that their 17-year-old son is missing. The boy has a chronic condition requiring regular treatment in hospital. The police request information from a hospital to ascertain if he has been admitted as a result of failure to take his medication. The hospital would be permitted, but not obliged, to provide this information under this provision.

## 11.2.7 Investigating and reporting wrong conduct

### HPP 10(1)(h) and 11(1)(i)

A health service may use or disclose personal health information if the health service has reasonable grounds to suspect that there has been or there is the possibility of unlawful activity, unsatisfactory professional conduct or professional misconduct under health registration legislation or conduct by a staff member that may be grounds for disciplinary action. Disciplinary policies should be followed when using or disclosing personal health information for these purposes. Staff and patients should be made generally aware in staff contracts/ patient leaflets that information about them may be subject to such uses and disclosures.

The exemption allows use or disclosure of the information necessary for the health service to investigate or report the conduct in question. It covers but is not limited to information to be provided to:

- the Health Care Complaints Commission
- NSW Health Professional Council or National Board information or
- units of the NSW Ministry of Health which may conduct investigations into breaches of legislation, including the Pharmaceutical Services Unit (NSW Ministry of Health)
- investigative units within NSW Health

#### 11.2.7.1 Public Interest Disclosures

When examining reports of wrong conduct, consideration should be given to whether the report may be considered a Public Interest Disclosure (PID) under the provisions of the [Public Interest Disclosures Act 2022](#). Reports of wrongdoing in a privacy related

matter may relate to corrupt conduct or a government information contravention. Reports of wrongdoing made by public officials can attract the provisions of the [Public Interest Disclosures Act 2022](#) and should be referred to the PID co-ordinator or Chief Executive for consideration.



#### Further guidance:

- [Public Interest Disclosures \(PD2023\\_026\)](#)
- Section 4.3.4 Disciplinary matters and ICAC reporting

## 11.2.8 Law enforcement agencies, including police

### HPP 11(1)(j)

HPP 11 allow health services to disclose personal health information to law enforcement agencies. In order to do so:

- the disclosure must be reasonably necessary to the functions of the law enforcement agency
- there must be reasonable grounds to believe that an offence may have been or may be committed.

#### 11.2.8.1 What is a 'law enforcement agency?'

The [Health Records and Information Privacy Act 2022](#) recognises the following agencies as law enforcement agencies:

- NSW Police or the police force of another State or a Territory
- Australian Federal Police
- NSW Director of Public Prosecutions (or equivalent office in another State, Territory or the Commonwealth)
- NSW Crime Commission
- Australian Crime Commission
- Corrective Services NSW
- Youth Justice NSW

#### 11.2.8.2 What sort of information can be provided?

The law enforcement exemption under HPPs 10 and 11 is very broad. It covers any health information relating to an offence which has or may be committed, provided that the information is 'reasonably necessary' to assist the law enforcement agency to perform its functions.

This exemption does **not oblige** health services to supply the information. Health services need to balance the important public interest in assisting law enforcement agencies to pursue their law enforcement and public protection functions with their own obligations of confidentiality to their patients and the sensitive nature of health information.

Generally, the information supplied should be limited to confirmation of identity and address.

The only exception is where the police can confirm they are actively investigating the commission of an offence and that the information is 'essential to the execution of their duty'. In such circumstances, there may sometimes be situations where additional, limited clinical information can be provided to the police, where appropriate. Careful consideration should be given to additional information provided, having regard to:

- The seriousness of the offence involved. For example, does it involve an offence involving serious physical harm, such as attempted murder or assault?
- The level of public risk. Is there an ongoing public risk or risk to particular individuals that would be addressed by the health service providing information (this also falls into HPP 11(1)(c), Disclosure to address a serious threat to health or welfare – see Section 11.2.3).
- The impact of the disclosure on patient care and the therapeutic relationship. The nature of the service being provided and the potential that the patient may discontinue obtaining care and treatment, should be considered, as well as the possible impact on the patient's mental state or wellbeing.

In some other circumstances, NSW Health policy may require reporting of a criminal offence or other conduct to the police or another agency. The NSW Health policy directive [Domestic Violence – Identifying and Responding \(PD2006\\_084\)](#) states that in certain circumstances health staff must report to the police, regardless of the wishes of the victim. These circumstances may involve the victim sustaining serious injuries such as broken bones; the perpetrator having access to a weapon and is making threats; or if there is an immediate risk to public safety or health staff are threatened.

After considering these matters, if a health practitioner decides it is appropriate to provide additional information, consultation should first occur with a more senior health care provider. Depending on the nature of the request, staff may also seek advice from the Privacy Contact Officer or a senior health service manager.

Other health information may only be provided with patient consent or in response to a search warrant or subpoena (see Section 11.3.6 Search warrants and subpoenas).



### Further guidance:

- Section 11.3.4 Reporting 'serious criminal offences'
- Section 15.2 Requests from State and Federal Police

#### 11.2.8.3 Certificate of expert evidence

Evidence in court cases is generally provided verbally, through sworn evidence from each witness from the witness box, or via video link. Most witnesses to a court hearing will be lay witnesses. Lay witnesses (also known as a factual witness) will provide evidence of factual matters, on what they saw, heard or did.

Before a hearing, lay witnesses may voluntarily provide a written statement usually to a lawyer for the person who wants you to give evidence, outlining the facts known to that witness that is relevant to the court case. There is no obligation to provide a written statement. A lay witness is only allowed to provide relevant factual evidence. Witness statements are served on the parties to the court case, allowing each party the opportunity to prepare their cases. If a person provides a statement, they may be required to make themselves available to testify at the hearing. If a lay witness does not provide a statement, then that person may possibly be served with a subpoena ordering the person to attend Court. However, whilst this is possible it would be unusual. Lay witnesses are not to be allowed to provide their opinion on a matter.

An expert witness is a person who has specialised knowledge based on their training, study or experience. Unlike lay witnesses, an expert witness with specialist knowledge may express an opinion on matters within his or her area of expertise. Expert witnesses may provide information like a report, or a statement detailing their opinion on a patient's medical record, or an opinion on a topic that is within their expertise. For example, an expert witness can assess a patient and provide a report on their assessment and provide an opinion, for example on the mental condition of a patient. Or an opinion on whether a patient's actions could have been involuntary at a particular time. Or a report on the properties of a particular drug and its likely effect on the patient. Unlike a lay witness statement, expert witnesses must include in an expert certificate that describes their knowledge based on his or her training, study or experience and an opinion that is based on their specialist knowledge based on his or her training, study or experience. The *Evidence Act 1995* provides guidance on how the certificate should be drafted.

A request for a certificate of expert evidence is not a subpoena, search warrant or court order, and a health service is therefore not obliged to provide it nor does privacy law automatically 'authorise' release in this form. Therefore caution should be exercised prior to release, particularly where the doctor is no longer employed or is not otherwise available to review the patient's records on site prior to compiling the certificate. In circumstances where the health service decides to send patient records off-site to a doctor for review, these should be password protected (or de-identified, with the patient's identity provided to the doctor separately). Consideration of the public interest balanced with patient privacy should be made as described above (see Section 11.2.8.2 What sort of information can be provided?).

#### 11.2.8.4 How should requests from law enforcement agencies be handled?

Requests should be in writing on letterhead or via email, identifying the requesting officer, providing full address and contact details, and confirming the officer is a representative of a law enforcement agency. The request should also indicate the reason why the law enforcement agency is seeking the information.

Information should not generally be provided by telephone unless in response to a written request or where the requesting officer's identity can be verified.

Requests should be dealt with by the treating health care provider, a senior health professional or a health information manager. When information is provided the service provider should:

- limit access to information that is directly relevant to the inquiry and clearly necessary for the purpose
- document all instances of access in the health record (including any written requests from police)

#### Example

A paramedic attends a patient being held in a police holding cell. After the patient has been examined, the police officer asks questions about the patient relating to their health, and whether in the paramedic's opinion the patient is medically competent to be interviewed. The paramedic should only disclose information relating to the patient which is necessary to enable the police to monitor the condition of the patient, including symptoms which would require the patient to be taken to hospital. Paramedics are not required to discuss other matters relating to the patient, such as whether the patient is medically competent to be interviewed.

- where clinical information is necessary, this should be limited to a general outline of the patient's condition and/or injuries.

#### 11.2.8.5 Law enforcement requests in emergency circumstances

Where a health service receives a request for patient information which is urgently required to assist a law enforcement agency with an investigation, and it is impractical or unreasonable to receive this request in writing prior to disclosure, the senior treating clinician may provide limited patient information to the law enforcement agency verbally in person or via telephone.

Prior to release of information, the senior treating clinician must verify the caller's identity. This will require the requesting officer to provide their name, rank and command contact details (or equivalent). The senior treating clinician should then contact the command to confirm the caller's identity and be transferred to that officer.

The scope of the information provided to the law enforcement agency should be consistent with Section 11.2.8.2.

NSW Health has developed a protocol in partnership with NSW Police to assist staff with the sharing of personal health information following a serious motor vehicle accident. This protocol is titled '[NSW Police Force Crash Investigation Injury Assessment Protocol](#)'.

Other circumstances recognised by the [Health Records and Information Privacy Act 2002](#) which may involve an emergency response are:

##### 1. 'Serious and imminent threat'

Disclosure of personal health information is permitted where the health service has reasonable grounds to believe this is necessary to lessen or prevent a serious and imminent threat to the life, health or safety of a person, or a serious threat to public health or public safety (see Section 11.2.3).

##### 2. 'Finding a missing person'

Disclosure of personal health information is permitted to ascertain the whereabouts of a missing person reported to the police (see Section 11.2.6).

##### 3. 'To assist in the stage of an emergency'

Use or disclosure of personal health information is permitted to assist in a 'stage of emergency' as defined in the [State Emergency and Rescue Management Act 1989](#) (fire, flood natural disaster, for example) (See Section 11.2.4).



## Further guidance:

- Section 11.2.8.2 – What sort of information can be provided?
- Section 11.2.3 – To prevent a serious and imminent threat to health or welfare
- Section 11.2.6 – Finding a missing person
- Section 11.3.4 – Reporting ‘serious criminal offences’
- Section 11.3.7 – Search warrants and subpoenas
- Section 15.2 – Requests from state and federal police

### 11.2.9 Investigative agencies

#### HPP (10)(1)(j) and HPP (11)(1)(k)

The [Health Records and Information Privacy Act 2002](#) permits sharing of patient health information for the purpose of complaint handling or investigative functions by investigative agencies. A health service may use or disclose personal health information if this is **reasonably necessary** to the complaint handling or investigation functions of an investigative agency.

Under privacy law, an investigative agency is:

- the Ombudsman’s Office
- the Independent Commission Against Corruption (ICAC) and the Inspector of ICAC
- the Law Enforcement Conduct Commission (LECC) and the Inspector of the LECC and any staff of the Inspector
- the Community Services Commission
- the Health Care Complaints Commission
- the Office of Legal Services Commissioner
- the Ageing and Disability Commissioner
- the NSW Office of the Children’s Guardian
- any other person or body prescribed by Regulation for the purposes of the investigative agency definition.

In all cases where information is provided to an investigative agency, a health service must:

- as far as reasonably practicable, only respond to written requests which clearly set out the purpose for which the information is required and the provisions of the relevant Act under which the agency seeks the information
- seek and document proof that the person seeking the information is a representative of an appropriate investigative agency
- if in doubt about whether to supply the information, seek advice from the Health Information Service, Privacy Contact Officer or a senior manager

- provide access only to information that is relevant and necessary for the purpose
- document all instances of access in the health record
- where appropriate and practicable, inform the individual to whom the information relates of the access.

### 11.2.10 Disclosure on compassionate grounds

HPP 11(1)(g) and the [Health Records and Information Privacy Regulation 2022](#)

A health service may disclose relevant personal health information to an immediate family member for compassionate reasons. This only arises in relation to a ‘disclosure’ and will not apply to a use.

This exemption is generally intended to assist family members with understanding or coming to terms with events that have occurred to their close relative while in the care of the health service and understanding the circumstances of their death.

An immediate family member includes an individual person who is:

- a parent, child or sibling of the individual, or
- a spouse of the individual, or
- a member of the individual’s household who is a relative of the individual, or
- a person nominated to an organisation by the individual as a person to whom health information relating to the individual may be disclosed.

The exemption is restricted as follows:

- the disclosure must be limited to ‘what is reasonably necessary’ for those reasons; and
- the individual must be deceased or incapable of giving consent; and
- the disclosure must not be contrary to any wish the individual has expressed and has not withdrawn, that the health service is aware of or could reasonably make itself aware of.

Before disclosing on compassionate grounds, consideration should be given to any health and safety concerns.

Disclosure is limited to a reasonable extent for those compassionate grounds; therefore, it is important to make a careful assessment of what part of the patient’s health record is ‘reasonably necessary’ or ‘relevant’ to the family member making the request for access on compassionate grounds. As such, what will be reasonable will vary depending on the particular circumstances. For this reason, it may be appropriate to consult with treating clinical staff to identify the most appropriate types of information for disclosure.

For any requests for information on compassionate grounds, the health service should always ask the applicant if they are seeking information from multiple health services and districts as this can sometimes be more complex and requires special management as outlined in Section 11.2.10.2.

The purpose of the exemption is a compassionate one, and staff should consider that a 'compassionate' release of information may still be appropriate when family members are in dispute about access to information. Guidance can be sought from the Ministry of Health privacy team.

Disclosure on compassionate grounds would not generally cover release of an individual's entire health record and the amount of information disclosed will need to be considered on a case-by-case basis. An individual who seeks access to the entire health record should be advised to make a request for access under either the [Health Records and Information Privacy Act 2002](#) or the [Government Information \(Public Access\) Act 2009](#) (see Section 12 Patient access and amendment (HPPs 6, 7 and 8)), or otherwise to issue a subpoena via their legal representative. More guidance is provided below in 11.2.10.1.

Personal health information is covered by privacy principles until 30 years after a person has died. Relevant personal health information may be disclosed at any point in time under compassionate grounds. This may be relevant in circumstances where an immediate family member has been estranged and may want some information about a patient's death or illness some years after they have died.

If the immediate family member seeking access is under the age of eighteen, the health service must assess whether they have sufficient maturity to receive the information.

If information is being released on compassionate grounds in circumstances where a patient has died some time ago and a family member is requesting information after a significant lapse of time, there should be some evidence provided that the requesting party is an 'immediate family' member. This could be a birth certificate or marriage certificate linking the deceased with the requestor.

#### **11.2.10.1 Releasing information to families for legal claims after a patient has died**

Health services may receive requests from solicitors and family members to access records in situations where the release of the deceased's records is clearly for the purposes of litigation. In such cases, disclosure is generally not permitted on compassionate grounds. The most appropriate channel for access is through a GIPA Act application or court order.

However, in circumstances where an executor of the deceased's estate makes a request for access, the information may be disclosed under the principle of

'lawful excuse'. Executors are appointed under a will and recognised under the *Probate and Administration Act 1898* (NSW), and have legal responsibilities to manage and finalise the affairs of the estate. Where an executor can demonstrate that access to the deceased's health information is reasonably necessary to fulfil their legal duties, disclosure may be permitted on that basis.

It should be noted that lawful excuse applies only to access for estate administration purposes and does not entitle an executor to act more broadly on the deceased's behalf. For example, an executor is not entitled to request amendments to a deceased person's health record.

Further advice can be sought from Privacy and GIPA Officers.

#### **Example**

1. A young person is admitted to hospital unconscious and seriously ill, they have no identification, but their mobile telephone address book includes an entry for 'Mum at home'. You may contact the mother and inform her of her son's admission and general medical state.
2. A person has died suddenly at hospital without indicating his wishes to staff about how his personal health information should be dealt with. Two of the person's daughters, aged 15 and 17 arrive in a distressed state and wish to know the cause of death. In such case, the information could be shared with them, provided you have assessed they are sufficiently mature to cope.
3. A person with a history of drug use has died in hospital after a long AIDS-related illness. Before dying she has told hospital staff, she does not want her family to know the cause of death, as she had kept her drug use a secret. The family arrive and wish to know the cause of death. In such a case, you would be able to give only limited details.
4. A parent has died in hospital and one of their three adult children has been estranged from the family for some time. The other two children (who were on good terms with their parent) do not want their estranged sibling to have any information about their parent's death. The estranged child has contacted the hospital to find out what happened to their parent and the cause of death. Provided the parent did not express any wish to withhold information from the estranged child prior to their death, the hospital would be able to release limited details to the estranged child about their parent's illness and death, even if this was contrary to the wishes of the other two children.

### 11.2.10.2 Compassionate release involving multiple health services

Some patients have complex and chronic health needs that are managed across multiple health services and Local Health Districts.

In the event of the patient's death (or incapacity), immediate family members may seek access to the patient's health care records on compassionate grounds to gain some closure or understanding.

It can be frustrating and confusing for family members when health services and districts have different processes for the disclosure of information on compassionate grounds. Sometimes this can be because the deceased or incapacitated relative gave strict instructions to one District about the management of their records but gave no restrictions on access to records in other Districts where they were treated.

Where matters like this arise and a patient had clinical care across multiple Districts, it is recommended that the Ministry of Health privacy team be consulted on coordinating responses to the family. This will assist in ensuring consistent approaches that accurately reflect the wishes of the deceased (or the patient who does not have capacity) and other relevant considerations.

This may also have relevance in cross-border communities where patients sometimes seek treatment across different states and territories for different health services.

### 11.2.11 Chaplaincy services

Chaplaincy services are considered an important part of the health support services provided through hospitals and other health services to patients and their families. Chaplaincy services are provided by trained accredited chaplains and trained accredited pastoral care workers (including volunteers) who are required to comply with privacy legislation. A regulation under the [Health Records and Information Privacy Act 2002](#) allows information to be provided to an accredited chaplain or pastoral care worker where this is a 'reasonable expectation' of the patient. The [Privacy Leaflet for Patients](#) informs patients that information about them may be provided to accredited chaplains and pastoral care workers.

Typically, a patient list is provided to accredited chaplains and pastoral care workers (including volunteers). This generally includes patient's name, religious affiliation (if this is provided to the health service) and ward location. Patient lists should only be released to accredited chaplains and pastoral care workers.

Further information about the patient's health care and treatment can also be disclosed to the accredited chaplain or pastoral care worker (including volunteers) involved in the patient's care where this is considered by the treating team to be relevant and appropriate.

With agreement from treating clinical staff, accredited chaplains and pastoral care workers may document significant pastoral and spiritual care intervention in the patient's health record. Further guidance is available in the [NSW Health and Civil Chaplaincies Advisory Committee NSW Memorandum of Understanding \(PD2011\\_004\)](#).

The patient may indicate at any time if they do not wish to receive chaplaincy services or if they do not want their information to be made available to accredited chaplains and pastoral care workers (including volunteers). The health service must ensure these wishes are complied with.



#### Further guidance:

- [NSW Health and Civil Chaplaincies Advisory Committee NSW Memorandum of Understanding \(PD2011\\_004\)](#)
- NSW Health [Privacy Leaflet for Patients](#)

## 11.3 Use and disclosure authorised by law – HPPs 10(2) and 11(2)

Privacy law recognises that there are many cases where a use or disclosure of information is either allowed by another law or is required by that law.

Where an agency seeks access pursuant to a lawful authorisation, the health service should:

- request written confirmation from the agency of the request and its legal basis
- provide only the information required by the authority
- check whether [Health Records and Medical/Clinical Reports – Charging Policy \(PD2006\\_050\)](#) applies to the request.

If there are doubts about the relevance of the documents to the purpose described in the law, staff should seek a written confirmation of relevance from the agency exercising their statutory power.

It is necessary to confirm not only that the requesting agency holds the legislative authority to require the information to be provided, but also that the circumstances set out under the relevant legislation apply to the case in question.

There are many such statutes, but some examples of those which commonly apply to a health service are set out below.

### 11.3.1 NSW Ministry of Health Officers and Environmental Health Officers

NSW Ministry of Health officers have powers under the [Health Services Act 1997](#) and the [Private Health Facilities Act 2007](#) to obtain information. Inspectors carry authorisations that indicate the nature of their powers and confirm their authority.

Section 42 of the [Poisons and Therapeutic Goods Act 1966](#), allows an officer of the NSW Ministry of Health to be appointed as an 'inspector' with powers to inspect and make copies of records relating to regulated goods, including records containing personal health information.

Environmental Health Officers from Public Health Units have powers under the [Public Health Act 2010](#) to obtain information. Inspectors carry authorisations that indicate the nature of their powers and confirm their authority.

### 11.3.2 Child protection

The information provided in this section is intended to provide a summary of the key issues relating to the balance between privacy and confidentiality and child protection. Details are provided in the following resources:

- [NSW Health Prevention and Response to Violence, Abuse and Neglect \(PARVAN\)](#)
- [Child Wellbeing and Child Protection Policies and Procedures for NSW Health \(PD2013\\_007\)](#)
- [Child Protection Counselling Services Policy and Procedures \(PD2019\\_014\)](#)
- [Child Wellbeing and Child Protection – NSW Interagency Guidelines for Practitioners](#)
- [NSW Interagency Mandatory Reporter Guide](#)

#### Chapter 16A

Chapter 16A of the [Children and Young Persons \(Care and Protection\) Act 1998 \(Care Act\)](#) takes precedence over other laws regulating the disclosure of personal information, such as the [Privacy and Personal Information Protection Act 1998](#) and the [Health Records and Information Privacy Act 2002](#). Under Chapter 16A, each district is considered a separate prescribed body, rather than one single entity.

Chapter 16A provides for certain agencies, generally those working with children and families classed as 'prescribed bodies' under the [Children and Young Persons \(Care and Protection\) Act 1998](#), to exchange information with other prescribed bodies relating to a child's or young person's safety, welfare or wellbeing in certain circumstances.

Section 245B(3) of the [Children and Young Persons \(Care and Protection\) Act 1998](#) provides that Chapter 16A also applies to safety, welfare or wellbeing information relating to an unborn child who is the subject of a prenatal report (section 25) or a referral to a [NSW Health Child Wellbeing Unit](#) (section 27A). If a Health worker is unsure whether any report or referral has been made during the pregnancy, they can contact the NSW Health Child Wellbeing Unit for advice or, if after hours, the Child Protection Helpline.

Under Chapter 16A, information relating to the safety, welfare or wellbeing of a child or young person (including an unborn child who is the subject of a prenatal report) can be shared between prescribed bodies if the information is necessary to:

- inform any decision, assessment or plan or to initiate or conduct any investigation, or to provide any service, relating to the safety, welfare or well-being of the child or young person or class of children or young persons, or
- manage any risk to the child or young person (or class of children or young persons) that might arise in the recipient's capacity as an employer.

A prescribed body for the purposes of Chapter 16A includes:

- the NSW Police Force
- a NSW government department or NSW public authority, including the Department of Communities and Justice (DCJ)
- a NSW government school or a NSW registered non-government school
- a NSW TAFE
- a NSW public health organisation or a NSW licensed private health facility
- a DCJ-accredited or DCJ-registered out-of-home care agency
- a DCJ-accredited adoption service
- the Family Court of Australia, the Federal Magistrate's Court of Australia, Centrelink and the Department of Immigration and Border Protection
- any other organisation which has direct responsibility for, or direct supervision of, the provision of health care, welfare, education, children's services, residential services, or law enforcement, wholly or partly to children
- nurses, medical practitioners, midwives, occupational therapists, psychologists and speech pathologists eligible for membership of Speech Pathology Australia.

Further information relating to Chapter 16A, including how to respond to requests and what to do if information is not to be provided, can be found in the relevant NSW Health policies.



### Further guidance:

- [Child Wellbeing and Child Protection Policies and Procedures for NSW Health \(PD2013\\_007\)](#)
- [Responding to Sexual Assault \(adult and child\) Policy and Procedures \(PD2020\\_006\)](#)
- 12.5.3 Reports to the Department of Communities and Justice (DCJ)

#### Section 248

Section 248 of the [Children and Young Persons \(Care and Protection\) Act 1998](#) allows for the exchange of information relating to the safety, welfare and wellbeing of a child or young person between DCJ and a prescribed body.

While generally DCJ will use Chapter 16A to request information relating to child protection, in some situations DCJ will require a prescribed body to provide information to them. If a section 248 request is made for personal health information to be provided, a NSW Health agency must comply with the direction. The information must be directly relevant to safety, welfare and well-being of a particular child or young person or class of children or young persons. Information can usually be provided by way of an extract from the health record. Full health records are not normally provided.



### Further guidance:

- [Child Wellbeing and Child Protection Policies and Procedures for NSW Health \(PD2013\\_007\)](#)
- [Children and Young Persons \(Care and Protection\) Act 1998](#)

#### 11.3.2.1 Reporting children and young people at risk of significant harm

Under section 24 of the [Children and Young Persons \(Care and Protection\) Act 1998](#), a person who has reasonable grounds to suspect that a child or young person is at risk of significant harm may make a report to DCJ.

Under section 27 of the [Children and Young Persons \(Care and Protection\) Act 1998](#) health staff must make child protection reports to DCJ where they have reasonable grounds to suspect that a child or young person is at risk of significant harm to DCJ, or to the NSW Health Child Wellbeing Unit Under section 27A.

Under section 25 of the [Children and Young Persons \(Care and Protection\) Act 1998](#), health staff who have reasonable grounds to suspect, before the birth of a child, that the child may be at risk of significant harm when born may make a pre-natal report to DCJ.

Staff should use the online [NSW Interagency Mandatory Reporter Guide](#) to assist in determining whether a report to the Child Protection Helpline or to the NSW Health Child Wellbeing Unit is indicated.



### Further guidance:

- [NSW Mandatory Reporter Guide](#)

#### 11.3.2.2 Protection for mandatory reporters

Section 29 of the [Children and Young Persons \(Care and Protection\) Act 1998](#) provides for the protection of persons who make reports or provide certain information to DCJ or to the NSW Health [Child Wellbeing Unit](#).

Where access is being requested to reports made to DCJ, the identity of the staff member who made the report, or information from which the identity of that person could be deduced, is privileged and must not be disclosed, except with:

- the consent of the person who made the report,
- the leave of a court or other body before which proceedings relating to the report are conducted.

Where uncertainties exist regarding disclosure, or consideration is being made for the disclosure of the identity of a staff member who has provided information to DCJ, advice should be sought from a health information manager, Privacy Contact Officer or legal officer at the health service or NSW Ministry of Health.

#### 11.3.2.3 Protection for medical examinations

**Section 173:** Where a medical examination has been conducted in accordance with Section 173 of the [Children and Young Persons \(Care and Protection\) Act 1998](#), a written report of the examination may be disclosed to the Department of Communities and Justice or the police.

Reports made under section 173 should be provided without charge by health staff. A health practitioner who transmits a report prepared under these circumstances is protected under the [Children and Young Persons \(Care and Protection\) Act 1998](#) from legal action in relation to allegations of professional misconduct and defamation.

#### 11.3.2.4 Child Sexual Assault Medical Protocol: Sexual Assault Investigation Kit (SAIK)

The Child Sexual Assault Medical Protocol is the written protocol in the Sexual Assault Investigation Kit (SAIK). The SAIK includes consent to disclose SAIK records to DCJ and Police for medico-legal purposes. Chapter 16A of the [Children and Young Persons \(Care and Protection\) Act 1998](#) may still provide a basis of sharing this information outside the terms of the consent.

Special sensitivities arise in relation to SAIK records. Particular care should be given to each request for SAIK records to ensure that this information is not disclosed unless for a purpose permitted by the consent given at the time of the administration of the SAIK (or by another later consent) or where the request meets the requirements of Chapter 16A of the [Children and Young Persons \(Care and Protection\) Act 1998](#). If it is not clear that the purpose for release is permitted by the consent, further details regarding the purpose of the request should be sought.



#### Further guidance:

- [Child Wellbeing and Child Protection Policies and Procedures for NSW Health \(PD2013\\_007\)](#)
- [Child Wellbeing and Child Protection – NSW Interagency Guidelines](#)
- [Photo and Video Imaging in Cases of Suspected Child Sexual Abuse, Physical Abuse and Neglect \(PD 2015\\_047\)](#)
- See section 11.3.2
- See Information sharing under section 248 of the [Children and Young Persons \(Care and Protection\) Act 1998](#)

#### 11.3.2.5 Staff support

It is good practice for health staff to inform their supervisor or manager when they have received a disclosure from a child or young person, of reported abuse or neglect, to confirm an appropriate action plan or to inform their manager after they have taken relevant steps to respond to the child or young person. Child protection issues are complex and may raise both professional and personal issues for health staff. Informing a supervisor, Child Protection Coordinator or Child Protection Counselling Service, should issues arise, helps them to be aware that a staff member may need additional support, information or supervision. Health staff may also contact their Local Health District or Specialty Network for information about contacting the Local Health District Staff Counsellor or Employee Assistance Program (EAP).



#### Further guidance:

- [Child Wellbeing and Child Protection Policies and Procedures for NSW Health \(PD2013\\_007\)](#)
- [Child Wellbeing and Child Protection – NSW Interagency Guidelines](#)
- [NSW Interagency Mandatory Reporter Guide](#)
- [NSW Health Prevention and Response to Violence, Abuse and Neglect](#)

#### Contact

- [NSW Health Kids and Families](#) (02) 9391 9000
- [NSW Health Child Wellbeing Unit](#) 1300 480 420

For support and assistance in determining the level of risk of harm and how to respond to the needs of vulnerable children and young people.

#### 11.3.3 Disclosing health information of custodial patients

Sharing of custodial patient health information between Justice Health and Forensic Mental Health Network (Justice Health NSW) and Corrective Services NSW/Youth Justice NSW is detailed in [Justice Health NSW Guideline: 'Guidelines on use and disclosure of health information' \(GL9.036\)](#). The Guidelines describe the circumstances where disclosure is authorised or required by the [Crimes \(Administration of Sentences\) Regulation 2014](#) (adults in custody) or the [Children \(Detention Centres\) Regulation 2015](#) (young people in custody). An example of a required disclosure under the [Crimes \(Administration of Sentences\) Regulation 2014](#) is found in clause 285, which provides that, where a health officer forms an opinion that the mental or physical condition of an inmate constitutes a risk to the life of the inmate, or to the life, health or welfare of any other person, the health officer must report that he or she has formed that opinion and the grounds of the opinion to a Corrective Services NSW officer.

Justice Health NSW staff may disclose relevant information on the medical history or status of a custodial patient to Corrective Services NSW/Youth Justice NSW to investigate an incident or assault involving that patient where the law enforcement exemption applies (see Section 11.2.8). Requests should be in writing indicating the basis for disclosure. Consent from the patient must be obtained, unless other lawful disclosure applies (for example, risk of harm, see Section 11.2.3, or law enforcement, see Section 11.2.8).



#### Further guidance:

- [Justice Health NSW Guideline: 'Guidelines on use and disclosure of health information' \(GL9.036\)](#)

### 11.3.4 Reporting ‘serious criminal offences’ and ‘child abuse offences’

Section 316 of the [Crimes Act 1900](#) requires a person to consider whether the information they have will be of ‘material assistance’ to securing the apprehension or conviction of a person for a ‘serious criminal offence’. If it is, they are obliged to notify police. Failure to do so could lead to a conviction and the imposition of a penalty of up to 5 years imprisonment if there is no ‘reasonable excuse’ for this failure.

A ‘serious criminal offence’ is defined as an offence which attracts a penalty of five years imprisonment or more. Health staff should be aware that this covers offences such as drug trafficking, serious assaults, sexual assaults, murder and manslaughter. It does not cover minor drug possession offences or any offences under public health legislation.

The Regulations under the [Crimes Act 1900](#) also provide that prosecution for an offence under section 316 will not be commenced against a person without the approval of the Director of Public Prosecutions if the information was obtained in the course of practising as a:

- medical practitioner
- psychologist
- nurse
- legal practitioner
- social worker, including, a support worker for victims of crime, and a counsellor who treats persons for emotional or psychological conditions suffered by them.

The aim of the provision is to protect health care providers who, in good faith and on reasonable grounds, do not disclose this information to police.

Section 316 of the [Crimes Act 1900](#) also provides that there is a reasonable excuse for not reporting to police if:

- the information relates to a domestic violence offence or sexual offence against an alleged victim, and
- the alleged victim was an adult at the time the information was obtained by the person, and
- the person believes on reasonable grounds that the alleged victim does not wish the information to be reported to the police.

There is also a specific offence at s316A of the [Crimes Act 1900](#) relating to concealing child abuse offences.

Section 316A of the [Crimes Act 1900](#) requires a person to consider whether the information they have will be of ‘material assistance’ to securing the

apprehension or conviction of a person for a ‘child abuse offence’. If it is, they are obliged to notify police. Failure to do so could lead to a conviction and the imposition of a penalty of up to five years imprisonment if there is no ‘reasonable excuse’ for this failure.

The concealment of a child abuse offence includes concealment of a variety of sexual offences, serious assaults, and the failing of parental responsibility for a child. It has a maximum penalty of imprisonment for five years where the maximum penalty of the underlying child abuse offence is 5 years or more.

A person will not be guilty of the offence, however, if they have a reasonable excuse for not reporting the information to Police. This is similar to the existing requirement to inform Police of a serious indictable offence (section 316 of the [Crimes Act 1900](#)). Reasonable excuses for not reporting information to Police include knowing or reasonably believing that:

- the information has already been reported under mandatory reporting obligations, such as to the Child Protection Helpline, NSW Health Child Wellbeing Unit or to the Ombudsman under the Reportable Conduct Scheme, or the person believes on reasonable grounds that another person has reported it
- the information is already known to Police
- the victim is an adult at the time of providing the information and doesn’t want it reported to the Police, or
- there are grounds to fear for their safety or another person’s safety if they report to Police.



#### Further guidance:

- Section 11.2.8 Law enforcement agencies, including police
- [NSW Health Policy Directive Domestic Violence – Identifying and Responding \(PD2006\\_084\)](#)
- [Information sharing for service coordination, Department of Communities and Justice](#)

### 11.3.5 [Crimes \(Domestic and Personal Violence\) Act 2007](#)

Section 98M of the [Crimes \(Domestic and Personal Violence\) Act 2007](#) provides that an agency may, despite the privacy legislation, deal with information about a person without the consent of the person in certain circumstances.

Part 13A of the [Crimes \(Domestic and Personal Violence\) Act 2007](#) enables information to be shared without consent in some circumstances. It indicates

that if consent is not provided by the person, or it is unreasonable or impractical to obtain consent, health services are permitted to share information under part 13A with [Safer Pathway Local Coordination Points](#) or other domestic violence support services, including NSW Police.

If disclosure is made under part 13A of the [Crimes \(Domestic and Personal Violence\) Act 2007](#), the risk must be serious, but there is no requirement of imminent risk.

Further guidance on information sharing under part 13A is set out in the [NSW Government's Domestic Violence Information Sharing Protocol](#). The Information Sharing Protocol's chapter on serious threat provides more detailed guidance to support service providers' decision making on sharing information without consent.

Section 13 of the [NSW Government's Domestic Violence Information Sharing Protocol](#) outlines details about sharing information where a serious threat is identified and provides guidance to support decision making where consent to share information is not provided. For further information about NSW Health's approach to managing disclosures under the [Crimes \(Domestic and Personal Violence\) Act 2007](#), see the NSW Health Policy Directive [Domestic Violence Routine Screening \(PD2023\\_009\)](#).

[NSW Health Information Bulletin, Use of Exchange of Information Part 13A Crimes \(Domestic and Family Violence\) Act 2007 Form \(IB2016\\_056\)](#) provides assistance for NSW Health workers to comply with requirements under the [Crimes \(Domestic and Family Violence\) Act 2007](#).



#### Further guidance:

- [NSW Health Policy Directive Domestic Violence Routine Screening \(PD2023\\_009\)](#)
- [NSW Health Information Bulletin, Use of Exchange of Information Part 13A Crimes \(Domestic and Family Violence\) Act 2007 Form \(IB2016\\_056\)](#)
- [NSW Government's Domestic Violence Information Sharing Protocol](#)

### 11.3.6 Coroner

The [Coroners Act 2009](#) requires notification to the Coroner of deaths occurring under certain conditions. The Coroner will require a copy of the health records and sometimes may require the original records. In such cases, the health service should take care to ensure a full copy of all documents is retained by the health service. This is important in the event the death occurs outside of normal business hours and clinical staff are requested by police, on behalf of the Coroner, to provide the patient health records rather than the Health Information Department, which has strict protocols around disclosure.

Health records required for postmortem examinations must be provided to the Coroner in a timely manner to enable the pathologist or medical officer conducting the postmortem.

Where a request or an order is made by the Coroner or the police for coronial purposes and it is some time after the death, the Coroner should provide a Notice to Produce requesting the clinical records. The Notice should be received on letterhead (or electronic equivalent) with reference to section 53 of the [Coroners Act 2009](#), and detailing the information required.

A Coroner may request a copy of the final Serious Adverse Event Review (SAER) report. In that event, the District/SHN should provide the report so that the Coroner is aware of any recommended system changes that are relating to the incident. However, the final SAER report cannot, however, be tendered in evidence. If lawyers have been engaged to represent the District/SHN, the panel firm should forward the SAER report to the Coroner using a standard pro-forma letter which alerts the Coroner to sections 210 and 21P of the [Health Administration Act 1982](#). If lawyers are not engaged, the LHD or SHN should provide a covering letter with the report noting that the SAER has been provided for information only and that pursuant to sections 210 and 21P of the [Health Administration Act 1982](#), it cannot be adduced or admitted in any proceedings.

For further information about the process involved with coronial requests, refer to the [Coroners Cases and the Coroners Act 2009 \(PD2010\\_054\)](#) and the [Incident Management Policy directive \(PD2020\\_047\)](#).



#### Further guidance:

- [Coroners Cases and the Coroners Act 2009 \(PD2010\\_054\)](#)
- [Incident Management Policy directive \(PD2020\\_047\)](#)

## 11.3.7 Search warrants and subpoenas

### Search warrants

Compliance with a search warrant is required by law and record keepers should inform their immediate supervisor of any official demand for such access to information. Where possible, a copy of the record should be made and retained by the health service.

### Subpoenas

Compliance with a subpoena is required by law. The return date should be noted on receipt and the subpoena dealt with promptly by the officer designated to co-ordinate responses to subpoenas.

Where a patient whose health record has been subpoenaed is not named as a party to the proceedings, they should be notified by the health service that the subpoena has been received and advised of the return date.

A subpoena may be challenged on a number of grounds including:

- abuse of process
- where the terms of a subpoena are excessively wide and imprecise, and to comply with them would be onerous
- public interest immunity
- legal professional privilege
- sexual assault communications privilege.

If a staff member has concerns about the scope of a subpoena, or considers it should be challenged, he or she should consult their immediate manager and obtain advice from the health service's solicitors, if appropriate.

Care should be taken that documents outside the scope of the subpoena are not provided by referring to the subpoena's schedule.

If acceptable, copies should be provided, and the original health record retained by the health service. Where originals are required, the health records should be forwarded to the Court and a complete copy kept by the health service.

Documents should be delivered to the Registrar or Clerk of the court in question by secure means, for example, courier delivery or registered post. A receipt signed by the official receiving the health record should be obtained which specifies the health record number, date received and name of the court. Some courts and tribunals accept subpoenaed material in an electronic format, such as on a USB device or via secure court portal. Where courts and tribunals (and other destinations external to NSW Health) do not have a secure portal, consideration should be given to sending any health information via eHealth's approved Secure File Transfer (SFT) service or other approved encryption services.



### Further guidance:

- [eHealth NSW secure file transfer](#)
- [NSW Health Policy Directive, Subpoenas \(PD2019\\_001\)](#)

## 11.3.8 Health Care Complaints Commission

### 11.3.8.1 Powers to enter premises

Authorised officers of the Health Care Complaints Commission (HCCC) have powers of entry that include the power to inspect, copy or remove health records and to require a person to provide information.

They carry authorisations that indicate the nature of their powers and confirm their authority. HCCC authorised officers can only exercise these powers with consent from the owner or occupier of the premises or with a search warrant.

### 11.3.8.2 Powers to obtain documents

Under sections 21A and 34A of the [Health Care Complaints Act 1993](#), the Health Care Complaints Commission also has powers to require the production of documents, in order to assist it in the assessment of a complaint, or as part of its investigations. Where the Commission exercises this power, it should provide a written order for the documents, citing the relevant provisions.

## 11.3.9 The Ombudsman

The Ombudsman is empowered to require health authorities to supply information where a formal investigation is being conducted under the [Ombudsman Act 1974](#).

## 11.3.10 Official visitors

Official visitors are appointed under the NSW [Mental Health Act 2007](#) to inspect declared mental health facilities.

Under Section 132 of the [Mental Health Act 2007](#), official visitors must be provided with access to health records relevant to the care of patients.

## 11.3.11 Domestic Violence Death Review Team and Child Death Review Team

Chapter 9A of the [Coroners Act 2009](#) provides for a Domestic Violence Death Review Team, to review deaths occurring in the context of domestic violence in New South Wales. Section 101L requires public service agencies and health professionals to provide full and unrestricted access to records to the Team that it requires to fulfill its functions.

The Child Death Review Team is established under Part 5A of the [Community Services \(Complaints, Reviews and Monitoring\) Act 1993](#). The NSW Child

Death Review Team and the Ombudsman review child deaths with the purpose of preventing and reducing child deaths. Under Section 34K of the [Community Services \(Complaints, Reviews and Monitoring\) Act 1993](#), the Child Death Review Team has powers to obtain unrestricted access to relevant health records and to obtain copies on request and it is the duty of public sector agencies to assist.

### 11.3.12 SafeWork NSW

Relevant sections of the [Work Health and Safety Act 2011](#) allow inspectors from SafeWork NSW (as the Regulator for the purposes of the Act) to require production of material relevant to the investigation of an alleged or possible breach of the Act. Such a request must usually be made either in writing stating the reasons why access is being sought, or a formal notice should be issued. Sections of the [Work Health and Safety Act 2011](#) relevant to the production or inspection of documents are:

- section 155 Powers of regulator to obtain information
- section 165 General Powers on entry (of an Inspector)
- section 171 Power to require production of documents and answers to questions
- section 174 Powers to copy and retain documents

### 11.3.13 NSW Ageing and Disability Commission

The purpose of the NSW Ageing and Disability Commission is to raise community awareness to reduce and prevent abuse, neglect and exploitation of older people and adults with disability. The Commission receives and responds to reports or allegations of abuse, neglect and exploitation of an older person or adult with disability. Under the [Ageing and Disability Commissioner Act 2019](#), the Commissioner has the power to conduct an investigation and for the purpose of the investigation to issue notices to produce documents or other things, and to apply for a search warrant. A public health organisation and a government sector agency may also provide relevant information to the Commission in accordance with the Act.



#### Further guidance:

- [NSW Health Information Bulletin, 'Ageing and Disability Commissioner' \(IB2020\\_006\)](#)

### 11.3.14 Commonwealth Agencies

#### 11.3.14.1 Commonwealth Department of Social Services

The Commonwealth Department of Social Services has powers under the [Social Security \(Administration\) Act 1999 \(Cth\)](#) to access information relating to pensions, benefits and allowances. The request must be in writing and notice must be given under Sections 192, 196 and 197 of the Act.

#### 11.3.14.2 Veterans' Affairs

Under Section 128 of the [Veterans' Entitlements Act 1986 \(Cth\)](#), the health service is required to release to the Department of Veterans' Affairs (DVA) relevant information relating to treatment received at any public health facility by repatriation beneficiaries.

Deaths of repatriation patients must also be reported to the DVA.

Disclosure of the names of DVA patients for the purpose of visits by voluntary groups, such as ex-service organisations, is only permitted with patient consent. Pro forma consent forms and information leaflets are available from the health service's DVA representative, or by contacting the [Government Relations Branch, Ministry of Health](#).

#### 11.3.14.3 Immigration and border protection – Illegal Non-Citizens

The Commonwealth Department of Home Affairs has powers under section 18 of the [Migration Act 1958 \(Cth\)](#) to obtain information about illegal non-citizens.

The power allows the Department of Home Affairs to require a health service to produce information believed to be relevant to ascertaining the identity or whereabouts of a person believed to be an illegal non-citizen. The power must be exercised by service of a notice in writing.

### 11.3.15 Statutory reporting requirements

The public health system is required to notify authorised agencies of certain types of personal health information. The following must be reported to the Ministry of Health:

- scheduled Medical Conditions and Notifiable Diseases
- inpatient statistics
- maternal and perinatal data for Perinatal Data Collection
- cancer cases (through the NSW Cancer Registry)
- congenital conditions (Register for Congenital Conditions).



### Further guidance:

- Section 15.9.6 Managing public health risks
- [NSW Health Admission Policy \(PD2017\\_015\)](#)
- [Notifying Cancer-Related Data to the NSW Cancer Registry \(PD2022\\_008\)](#)
- [NSW Register of Congenital Conditions – Reporting Requirements \(PD2018\\_006\)](#)
- [Notification of Infectious Diseases under the NSW Public Health Act \(IB2013\\_010\)](#)
- [Notifiable Conditions Data Security and Confidentiality \(PD2012\\_047\)](#)
- [Notification of Acute Rheumatic Fever and Rheumatic Heart Disease – the NSW Public Health Act 2010 \(IB2015\\_057\)](#)

### **Health Services Act 1997**

Chief Executives of health services have an obligation to report suspected unsatisfactory conduct or suspected professional misconduct of staff members or contracted service providers (VMOs) to the relevant health professional Council.

### **Adverse drug reactions**

Adverse drug reactions must be reported in accordance with the [Medication Handling Policy \(PD 2002\\_032\)](#).

### **Home and Community Care Act 1985 (Cth)**

The Commonwealth Home and Community Care (HACC) Program provides services that support older people to stay at home and be more independent in the community. The [Home and Community Care Act 1985 \(Cth\)](#) requires HACC service providers, which may include some NSW Health agencies, to operate within the reporting framework set out in their Aged Care Funding Agreement. This agreement requires the reporting of demographic and health details relating to individuals receiving HACC services.



### Further guidance:

- [Home and Community Care Minimum Data Set Version 2 – Collection and Reporting Requirements \(PD2008\\_050\)](#)

### **Poisons and Therapeutic Goods Act 1966**

The NSW Ministry of Health collects and maintains personal health information as required under the [Poisons and Therapeutic Goods Act 1966](#).

The [Poisons and Therapeutic Goods Act 1966](#) provides for the collection, use and disclosure of personal health information as follows:

- for the purpose of administering authorisations to prescribe drugs of addiction
- to the Medical Committee and its subcommittees for the purpose of advising on applications to prescribe drugs of addiction
- under the provisions of Section 43 of the Act when auditing and investigating individual health practitioners and licensed or authorised persons or organisations to ascertain compliance with the Act or Regulation.



### Further guidance:

- [NSW Health Pharmaceutical Services Unit](#)

## 11.3.16 Information required by the Minister or Premier

NSW privacy laws also recognise that from time to time the executive arm of government (for example, the Minister for Health and the Premier) may require access to and use of personal health information.

HPPs 10(4) and 11(4) therefore provide that nothing in the use and disclosure restrictions prevents the disclosure of personal health information by a public sector agency:

- to another public sector agency under the administration of the same Minister if the disclosure is for the purposes of informing that Minister about any matter within that administration; or
- to any public sector agency under the administration of the Premier, if the disclosure is for the purposes of informing the Premier about any matter.

### 11.3.16.1 Ministerial correspondence and briefings

NSW Health agencies are required to prepare correspondence and briefings for, and on behalf of, the Minister for Health, Minister for Mental Health and the NSW Premier as requested. Such requests may seek to include personal health information about the correspondent, or a person they claim to represent.

When responding to correspondence, staff should take care not to disclose personal health information other than that which has been provided by the correspondent, or with the consent of the patient, or as is necessary to appropriately address the concerns raised and provide relevant background information to the Minister.

Care should also be taken when responses are being prepared in consultation with more than one health service or district, to ensure that only relevant health information is accessible for the purpose of the response.

If the correspondent is seeking to obtain access to or a copy of their own health record, or that of a friend or relative, they should be referred to the Health Information Service, or equivalent, for the health service where the patient received health services (see also Section 12 Patient access and amendment).



#### Further guidance:

- Section 11.2.2.1 Where a third party seeks access

## 11.4 Computer systems and applications

Staff with access to NSW Health electronic applications, such as an electronic health record and the My Health Record, may only access, view and use or disclose information held in the system for purposes directly related to their work.

This means NSW Health staff may only view, access, use and disclose personal health information when it is necessary for them to do so to carry out their work duties, whether that be patient care or other work duties that require access to personal and health information like patient billing or human resource management.

If in doubt about their obligations, staff should seek advice from a senior manager, local Health Information Manager or Privacy Contact Officer.

Staff should be provided with the appropriate level of access to physical and electronic health records (for example, full, partial or no access) in accordance with their role and their work requirements. In compliance with NSW Health policies on information security, a secure physical and electronic environment must be maintained.

NSW Health electronic record systems are auditable so staff access can be reviewed following privacy complaints or because of systematic auditing.



#### Further guidance:

- Section 9 Retention, Security and Protection
- Section 16 Electronic Health Information Management Systems