Collection of health information

Health information must be collected directly from the patient, unless it is unreasonable or impracticable to do so. The information collected must be up to date, accurate, relevant and not excessive.

Reasonable steps must be taken to inform the patient about how the information may be used, who may access it and to whom it may be disclosed.

In particular, staff have an obligation to inform patients that their information may be shared with multiple staff and clinical services involved in their care.

The *Privacy Leaflet for Patients* must be made available to all patients.

Storage and security

Health information must be stored securely to protect from loss, and unauthorised access, use or disclosure. Health records must not be destroyed without permission. Approval should be obtained from the local Senior Records Officer.

Health information may be recorded in paper or digital formats. Staff should be aware of security risks when using mobile devices such as a USB, tablet, laptop or phone, including for photo, video or audio recording. Staff should ensure that mobile devices are password protected and securely stored when not in use. Staff must not use their personal mobile phones to take photos or make recordings, unless with approval from their manager and patient consent.

Health information should not be accessible to unauthorised people. Computers and other devices containing health information must be located in secure staff areas. If patient journey boards are viewable by the public, they should not display identifiable patient health information.

Emails containing health information should not be sent outside of NSW Health unless they are password protected or encrypted. Encryption of emails containing confidential information is recommended. Health information should only be emailed from NSW Health email addresses. Patient information must never be emailed from personal or university email addresses.

Staff may also make use of secure file transfer and secure messaging systems authorised for use by NSW Health, as an alternative to emails.

Staff should be mindful to protect confidentiality when discussing patient care via telephone, and in public areas, such as cafeterias and lifts

Access, amendment and accuracy

Patients or their authorised representatives can apply for access to, or amendment of, their health records. Applications should be in writing. Typically, such requests are handled by the Medical Records Department or Health Information Service. Fees may apply.

Clinical information systems

Clinical information systems include:

- Electronic medical records (eMR)
- Patient administration systems (PAS)
- Electronic pathology records
- Clinical registries for cancer and other diseases
- HealtheNet
- My Health Record

Clinical information systems are subject to the same strict privacy protections as paper records. Improper access is a very serious matter and may lead to disciplinary action or referral to police.

Staff are responsible for protecting log-in details. Passwords and other log-in details must never be shared. Information systems must never be accessible to unauthorised persons. Staff must log off immediately upon ending a session and computers should be locked during temporary time away.

HealtheNet

HealtheNet is a secure state-wide electronic record. It contains a summary of patient health information, for example, discharge summaries, pathology results, medication information, alerts and allergies. HealtheNet enables staff to access information from hospitals and community health facilities across NSW. HealtheNet also displays information contained in a patient's My Health Record.

My Health Record

My Health Record is Australia's national health record system. All Australians have a My Health Record, unless they choose not to have one. Patients can control the information included in their My Health Record.

Certain health information including discharge summaries and other key records are uploaded from HealtheNet to a patient's My Health Record. This allows the patient and healthcare providers to access these records wherever they are in Australia. Patients may request that their health information not be uploaded to their My Health Record.

Privacy complaints

If you receive a privacy complaint you must refer it to your agency's Privacy Contact Officer as soon as possible. You should also notify your Manager. It is important to deal with all complaints promptly.

A privacy complaint is an objection to the way personal or health information has been handled. For example, a person may complain that their health information has been inappropriately accessed or disclosed. A process of internal review is usually undertaken in response to a complaint

Further information

www.health.nsw.gov.au/patients/privacy
NSW Health Privacy Manual for Health Information
NSW Health Privacy Internal Review Guidelines
NSW Health Privacy Management Plan

NH700114 220819

Privacy Leaflet for Staff

How we protect health information

NSW GOVERNMENT | Health

Staff obligations

NSW Health is committed to safeguarding the privacy of patient and staff information.

Staff are bound by the NSW Health Code of Conduct and privacy legislation to maintain confidentiality of information accessed in the course of their duties. This includes not disclosing personal information about patients or staff on social media.

The *Health Records and Information Privacy (HRIP) Act 2002* (NSW) requires staff to protect the privacy of health information. The *Privacy and Personal Information Protection (PPIP) Act 1998* (NSW) requires staff to protect all other personal information, such as staff records.

The *HRIP Act* provides that **staff must not, other than in the course of their employment, intentionally disclose or use any health information** about an individual to which the staff member has access. Maximum penalty: $11,000 fine or imprisonment for 2 years or both. There is a similar offence under the *PPIP Act*.

Health agencies audit staff access to health records. Unauthorised access may lead to disciplinary action or referral to police. The *Crimes Act 1900* imposes penalties for unauthorised access to restricted computer data, such as electronic health records.

The *Independent Commission Against Corruption (ICAC) Act 1988* provides that corrupt conduct includes the misuse of information. Staff suspected of corrupt conduct may be reported to ICAC.

Privacy principles

Staff may access, use and disclose health information for the purpose of treatment and ongoing care, or as otherwise specified by the Health Privacy Principles.

Staff should refer to the NSW Health **Privacy Manual for Health Information** for detailed discussion of the Health Privacy Principles. The key principles are summarised below.

What is health information?

Health information is clinical and personal information relating to an individual. Typically this is all the information contained in a patient's health record, including the patient's name and contact details.

Use and disclosure of health information

Health information may be used or disclosed by staff for the purpose of providing treatment and care. In addition, health information may be used or disclosed for related purposes that would be reasonably expected for patient care.

It is standard practice to provide a patient's GP and other health care providers involved in ongoing care with a discharge summary. Where GPs or other providers request access to health information, it is important to ensure that only information relevant to the request is disclosed.

If a request is received to use health information for purposes unrelated to clinical care, it should be referred to the Health Information Manager or Privacy Contact Officer.

If a request is received more than 3 months after the patient's discharge, extra care must be taken. Either the request must be made in writing or the circumstances of the request must be fully documented. Refer to your Health Information Manager or Privacy Contact Officer for advice.

In addition, the Health Privacy Principles specify the circumstances in which health information may be used or disclosed for secondary purposes. These include:

- For statutory reporting to NSW and Commonwealth government agencies, for example, reporting Medicare details, notifiable diseases, births and deaths.
- To My Health Record, if the patient has one.
- In accordance with the Statutory Guidelines issued under privacy law for training purposes, management purposes, or research purposes.
- To conduct safety and quality improvement initiatives including patient satisfaction surveys.
- For purposes relating to organ or tissue donation. This may include sharing next-of-kin contact details.
- To help prevent a serious and imminent threat to someone's life, health or safety, or in an emergency.
- To provide access to Hospital Chaplains. Should patients wish their religion to be withheld from the chaplaincy service they must advise staff.
- To share information on the safety, welfare or wellbeing of children and young people in accordance with the *Children and Young Persons (Care and Protection) Act 1998*.
- To comply with a subpoena, summons or search warrant.
- For investigation and law enforcement purposes.

Police requests
Staff may confirm the identity and address of a patient with police provided certain requirements are met. As a general rule, police requests for information should be in writing. Verbal requests may be considered from police attending a health service in person (e.g. Crash Investigation Units, or serious criminal matters). Advice should be sought from the Health Information Manager or Privacy Contact officer before releasing patient information to police.

Special restrictions
Restrictions on use and disclosure apply to adoption, organ and tissue donation, sexual assault, drug and alcohol, sexual health and genetic information.

Child protection information also has restrictions; seek advice from your Child Protection Unit for local or interstate requests for information.

A patient's HIV information may be made available to clinical staff treating a patient for any condition, where clinically relevant. However, restrictions apply to how HIV information can be used for other purposes.

Consent for sharing information

Consent for the sharing of information should not be confused with consent for medical treatment. If you are not sure when consent is required contact your Health Information Manager or Privacy Contact Officer.

Staff must obtain consent when a use or disclosure of information is outside that which is allowed for by the *HRIP Act*, as described above. For example, consent will be required when health information is used for media or fundraising purposes, or for disclosure to a third party such as an insurer or employer who is not involved in the patient's care.

Consent for disclosure of health information can be provided either in writing or verbally and must be documented in the patient's health record.

Where appropriate, children aged 12 and over should be engaged in discussions about their own health care.

If a person, including a minor, does not have capacity to consent, an authorised representative can consent on their behalf. An authorised representative may be a guardian, family member, close friend or carer. If you are concerned about a patient's capacity to consent, consult with a clinician to confirm who can act as the patient's authorised representative.

A patient's carer may be included in healthcare discussions with patient consent, or when the carer is the patient's authorised representative. In these circumstances, the carer should be provided with information relevant to the patient's care and management.

Specialised services, including cancer, palliative care and mental health services, may share information in different ways with the patient, their carer, family members and the authorised representative. The *Mental Health Act* enables patients to nominate a designated carer who can receive patient information.