Storage and security

In paper and electronic formats, health information should be protected from loss, and unauthorized access, use or disclosure. Records must be stored securely and disposed of appropriately (secure bins and shredding).

Regardless of format, records containing health information must be stored securely and disposed of appropriately. Approval from the local Senior Records officer must be obtained prior to health record being destroyed. Health records must never be destroyed without permission.

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

Staff should be aware of security risks when using mobile devices such as a USB, smart phone, tablet or laptop. Staff should ensure that mobile devices are password protected and securely stored when not in use.

Emails containing health information should not be sent outside of NSW Health unless they are password protected or encrypted. 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.

Caution should be exercised when discussing patient details via telephone to ensure the caller has legitimate grounds to access the information requested. Care should be also taken to keep details to a minimum when leaving voicemail messages for patients.

Staff should be mindful to protect confidentiality when discussing patent care in public areas, such as cafeterias and lifts.

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. Discharge summaries, test results, medicines and imaging reports may be uploaded by staff to a patient's My Health Record. This allows the patient and healthcare providers to access these records wherever they are in Australia. Patients should be informed that they need to tell staff at the beginning of their visit if they do not want their health information to be uploaded to their My Health Record. My Health Record is the responsibility of the Australian Digital Health Agency.

Important Points

- All personal information and health information is confidential.
- Staff should ensure patient privacy is not breached if discussing patient cases and care in public areas, for example; cafeterias, lifts and corridors.
- Printers and faxes should be located in secure staff areas. Patient information should not accumulate around these.
- No personal health information should be given over the telephone, unless the caller has legitimate grounds to access the information and can give proof of identity. If in doubt, take the caller's telephone number and return their call, or ask that they send a fax or email displaying letterhead or signature to confirm the caller's identity and bonafides.
- Staff should not disclose patient information without delegated authority, authorisation from a manager or without patient consent.
- Fees and charges may be raised for provision of copies of health records.
- Database managers and custodians must ensure compliance with all privacy principles. Health records containing information pertaining to Adoption, Organ/ Tissue Donation, Child Protection, Sexual Assault, Genetic Information, Drug & Alcohol and Sexual Health have additional restrictions on use and disclosure.
- Staff can confirm the identity and address of a patient with police. Staff should obtain the police officer's name and telephone number before releasing patient information. Police requests should be in writing with patient consent where possible.

Remember

- Staff may only access patient/ employee personal or health information where this is required in the course of their employment, typically for the purpose of on-going patient care.
- Health facilities have an audit capacity in their electronic health records and other systems to investigate staff access to health records.
- Disciplinary action may be imposed if staff are found to be in breach of patient privacy, including the personal and health information of staff.

Further information is available at:

www.health.nsw.gov.au/patients/privacy

NSW Health Privacy Manual for Health Information

NSW Health Internal Review Guidelines

NSW Health Privacy Management Plan

SCHN Privacy Contact Officer:
Nadine Ghassibe
Nadine.ghassibe@health.nsw.gov.au
02 9845 2356

SCN160719 160719

Privacy Leaflet for Staff (SCHN)

How we protect health information

NSW GOVERNMENT

The Sydney children's Hospitals Network
care, advocacy, research, education

Staff obligations

NSW Health is committed to safeguarding the privacy of patient and staff information and has implemented measures to comply with these legal obligations.

Staff are required to comply with the Health Records and Information Privacy (HRIP) Act 2002 to protect the privacy of health information in NSW. Staff are also required to comply with the Privacy and Personal Information Protection (PPIP) Act 1998 which covers all other personal information, such as staff records.

Staff are also bound by the NSW Health Code of Conduct to maintain confidentiality of all personal and health information which they access in the course of their duties.

The HRIP Act provided 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 in the exercises of his or her official functions. Maximum penalty: $11/000 fine or imprisonment for 2 year or both. There is a similar offence under the PPIP Act.

Health agencies audit staff access to electronic health records. Unauthorised access to clinical information may lead to disciplinary action or referral to police. The Crimes Act 1900 imposes penalties for unauthorised access to restricted data held in computer, such as electronic health records. Database managers and data custodians are responsible for implementing privacy and security safeguards.

The Independent Commission Against Corruption (ICAC) Act 1988 provided that corrupt conduct includes the misuse of information that a public official, or former public official, has acquired in the course of his or her official functions. Staff suspected of corrupt conduct may be reported to ICAC.

Overview

This leaflet is to assist staff to meet their obligations in relation to health information. In summary:

- There are 15 Health Privacy Principles described below. Staff must comply with all principles.
- Staff should refer to the **NSW Health Privacy Manual for Health Information** for detailed discussion of each principle.
- **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 (see below).

What is health information?

Health information is personal and clinical information relating to an individual. Typically this is all the information contained in a patient's health record. Health information includes the patient's personal details such as name, address, contact details, date of birth and so on, as well as all of their clinical information including a patient's express wishes about the provision of health services.

Privacy complaints

If you receive a privacy complaint you must advise your Manager and/or the Health Information Manager for your facility. You must also notify the Privacy Contact Officer for your health service as soon as possible. **It is important to deal with all complaints promptly.**

A privacy complaint is an objection to the way a person's health or personal information has been handled. For example, a person may complain that the health service has inappropriately disclosed their information. Privacy legislation requires that, in most cases, a process of Internal Review be undertaken to investigate any written privacy complaint.

Use and disclosure of health information

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

It is not necessary to obtain patient consent to disclose relevant health information to another hospital, GP or to other clinicians or carers for the purpose of the patient's ongoing care.

It is standard practice to provide a patients' GP ad 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 the request is received more than 3 months after the patients 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 for advice.

Health Information may also be used or disclosed for certain related 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 research purposes approved by a Human Research Ethics Committee; for staff and student training purposes; or for planning, financial or management 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 welfare, 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 clinical staff or patient administrative staff.
- To share information about 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 Staff may confirm the identity and address of patients with police provided certain requirements are met. Requests from police must always be in writing. Staff should obtain the police officer's name and telephone number. Advice should be sought from Privacy Contact Officer or senior manager before releasing patient information to police.
- Some types of health information are subject to special restrictions on use and disclosure. There are special restrictions that apply to adoption, organ and tissue donation, child protection, drug and alcohol, sexual assault, sexual health, HIV and genetic information. Since 2017, the Public Health Act allows patient HIV information to be made available to all clinical staff treating a patient for any condition. Previously, HIV information was only available to staff directly involved in the treatment of HIV infection. Restrictions remain on how HIV information can be used for other purposes.
- If you receive a request for information relating to an interstate child protection matter you should seek advice from your Child Protection Unit.

Consent for sharing information

Consent for the sharing of information should not be confused with consent for medical treatment.

Staff must obtain consent when a use or disclosure of information is outside that which is allowed for by the HRIP Act. For example, consent will be requirement with 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 patients care.

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

If you are not sure when consent is required check with your manager, or contact your Health Information Unit or Privacy Contact Officer.

Collection of health information

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

Reasonable steps must be taken to inform the patient about how the information may be used and who may access it and to whom it will be disclosed. At the time health information is collected, staff have an obligation to ensure patients understand that sharing of information may subsequently occur to enable ongoing. The Privacy Leaflet for Patients must be made available to all patients.

Staff need to clearly information patients how they can expect their information to be shared. Specialised services, including cancer services, palliative care and mental health, may share information in different ways. It is especially important to inform patients who are being treated by multidisciplinary teams that their health information may be shared between different specialties or clinical services.