Storage and Security

Health information must be stored securely and hard copy information must be disposed of appropriately at all times using secure bins or shredding. It should never be put into unlocked bins.

In hard copy and electronic formats, health information should be protected from unauthorised access, use or disclosure. Health records and computer screens should not be accessible to unauthorised people. Printers and fax machines should be located in secure staff areas.

Caution should be exercised when discussing patient details via telephone to ensure the caller has legitimate grounds to access the information provided. Staff should ensure patient privacy is not breached if discussing patient cases and care in public areas, for example: cafeterias, lifts and corridors.

Ref. Privacy Manual for Health Information, Section 9 Retention, security and protection

Access, Amendment and Accuracy

Patients or their authorised representative can apply for access to their health records (including images). Applications for access or copies of health records should be in writing. Costs may apply. Some departments may have a procedure in place where sensitive or complex reports or health records are accessed with a doctor in the first instance. Staff should consider whether this is necessary before granting access. Patients are entitled to request amendment (not deletion) of their health information to ensure it is accurate, up to date and not misleading. Attachment of information provided by the patient is also permitted.

In addition to correct clinical information about a patient, their demographic information such as name, address, contact person and current GP details, must also be correct for each encounter.

Ref. Privacy Manual for Health Information, Sections 10 Accuracy and 12 Access and Amendment

Important Points

- All personal information and health information is confidential.
- Staff should not disclose patient information without delegated authority, authorisation from a manager or without patient consent.
- Care must be taken when collecting and storing health information on mobile devices, including USB, smart phones, laptops and so on. The Health Privacy Principles apply where a personal device is used to store images and health information.

Ref: Privacy Manual for Health Information, Section 9.2.2 Images and photography

- Database managers and data custodians are responsible for implementing appropriate privacy and security processes.

Ref: Privacy Manual for Health Information, Section 16 Electronic health information management systems

- 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.

Ref: Privacy Manual for Health Information, Section 15.9. Information-specific laws and policies

- 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 appropriate.

Ref: Privacy Manual for Health Information, Section 11.2.7 Law enforcement agencies, including police

Remember

Staff may only **access** patient and employee personal or health information where this is required in the course of their employment.

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.

Section 68 of 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 in the exercise of his or her official functions. (Maximum penalty: 100 penalty units or imprisonment for 2 years or both). There is similar applicable legislation under the PPIP Act.

In addition, staff should be aware that there are criminal offences relating to the **unauthorised access and misuse** of electronic data in the Crimes Act 1900.

NSW GOVERNMENT | Health

Further information

http://www.health.nsw.gov.au/patients/privacy/Pages/default.aspx

Privacy Manual for Health Information

Privacy Internal Review Guidelines

Privacy Management Plan

Child Wellbeing and Child Protection Policies and Procedures for NSW Health

NSW Health & Civil Chaplaincies Advisory Committee NSW Memorandum of Understanding

NH700114 050416

Information Privacy Leaflet for Staff

NSW GOVERNMENT | Health

Health Service 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 employee records.

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

Guidance for staff on the *HRIP Act* is provided in the NSW Health Privacy Manual for Health Information. Guidance on the *PPIP Act* is provided in the NSW Health Privacy Management Plan. This leaflet is a summary of the requirements of these Acts and policies, with a focus on the protection of health information.

Staff are also bound by a strict code of conduct to maintain confidentiality of all personal and health information which they access in the course of their duties.

Important

Staff may only **access** patient and employee personal or health information where this is required in the course of their employment.

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.

Section 68 of 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 in the exercise of his or her official functions. (Maximum penalty: 100 penalty units or imprisonment for 2 years or both). There is similar applicable legislation under the *PPIP Act*.

In addition, staff should be aware that there are criminal offences relating to the **unauthorised access and misuse** of electronic data in the Crimes Act 1900.

Introduction

This brochure is to assist staff understand and comply with the legislative obligations under the *HRIP Act*. In summary:

- There are 15 Health Privacy Principles and staff must comply with all principles.
- The key principles are described in this brochure.
- Specialised services, including but not limited to, cancer services, palliative care and mental health, may have additional or different patient expectations or needs to address regarding information sharing.
- Personal health information and carer's information is released for statutory reporting to State and Commonwealth government agencies, for example, Medicare details, births and deaths, and notifiable diseases such as cancer and infectious diseases.

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 physical or mental health or a disability.
- A patient's express wishes about the provision of health services to him or her.
- Information relating to the donation of human tissue.
- Genetic information that may be predictive of the health of the patient, relatives or descendants.

If health information is stripped of information which can identify an individual, or from which a person's identity can reasonably be ascertained, then it is considered to be 'de-identified' information. Privacy laws do not apply to de-identified information.

Ref: Privacy Manual for Health Information, Section 5 (Key concepts)

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.

Ref. Privacy Manual for Health Information, Section 14 (Complaints handling)

Use and Disclosure

Health information may be used or disclosed by staff for the primary purpose of providing treatment and ongoing care. In addition, it may be used or disclosed for the purposes such as management, training or research activities, for investigation and law enforcement, or where there are serious and imminent threats to individuals and the public, sending a reminder to attend an appointment and in ways that would be reasonably expected for patient care and wellbeing.

It is not necessary to obtain patient consent to disclose health information to other clinicians involved in treatment of the patient. Staff have an obligation to ensure the patient understands that this disclosure will occur to enable continuous ongoing care. This may include, for example, the transfer of information to a GP, to another hospital, or health service or health professional involved in the patient's care. Personal health information may also be used or disclosed for the other related purposes, for example:

- For statutory reporting to State and Commonwealth government agencies, for example, reporting Medicare details, notifiable diseases, births and deaths.
- To comply with a subpoena, summons or search warrant.
- For purposes related to the operation of the NSW Health service, for example, funding, planning and to conduct safety and quality improvement initiatives.
- 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 contact patients regarding patient satisfaction surveys that evaluate and improve services.
- To other health services and authorised parties to help prevent a serious and imminent threat to someone's life, health or welfare, or in an emergency.
- 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*
- Hospital Chaplains may use relevant patient information to provide spiritual and pastoral care to patients with a nominated religion. Should patients wish their religion to be withheld from the chaplaincy service they must advise clinical staff or patient administrative staff.
- To investigate and report a complaint. This includes but is not restricted to complaints about patient care, staff conduct, information privacy, patient safety, or any incidents occurring in the health service.
- To manage a legal action or claim brought by the patient against the health service.

Ref. Privacy Manual for Health Information, Section 11 (Using and disclosing personal health information)

Consent

Staff must always obtain consent when it is required, for example, when health information is used for media or fundraising purposes, or for disclosure to a third party who is not involved in the patient's care. If you are not sure when consent is required check with your Manager or contact your Health Information Service or your local Privacy Contact Officer. Consent for disclosure of personal health information can be provided either in writing and placed on the patient's health record or verbally. If provided verbally, this must be clearly documented in the patient's health record.

Ref. Privacy Manual for Health Information, Sections 5.4 (Consent) and 11.2.2 (Where a third party seeks access)

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 relevant, up to date and accurate. 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.

It is important to inform patients who are being treated by a number of multidisciplinary teams that their health information may be shared between different specialities or clinical services. Particular care should be taken if information is to be shared between agencies as patient consent may be required.

The ***Privacy Leaflet for Patients*** must be made available to all patients. It explains when and how patient information may be used and disclosed.

Ref: Privacy Manual for Health Information, Section 7 (Collecting personal health information) and Appendix 5