PRIVACY INFORMATION FOR STAFF

1. Health Service Obligations

NSW Health is committed to safeguarding the privacy of patient and employee 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, (reference: ***NSW Health Privacy Manual),*** and
- *Privacy and Personal Information Protection (PPIP) Act 1998* which covers all other personal information, such as employee records, (reference: ***NSW Health Privacy Management Plan***).

This leaflet is a summary of the requirement of these Acts and policies, with a focus on the protection of health information. References to relevant policy documents are provided for further guidance where required.
Staff may only access patient/employee personal or health information where this is required in the course of their employment.

2. 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 may have additional or different patient expectations or needs to address regarding information sharing, for example, cancer services, palliative care and mental health services.

3. 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.
Further guidance: Privacy Manual, Section 5.3

4. Privacy Complaints

If you receive a privacy complaint you must advise your Manager or the Medical Record/Clinical Information Manager of your facility. The Privacy Contact Officer for your health service must also be notified as soon as possible. The Privacy Contact Officer for SESLHD is Dr Tony Sara. **It is important to deal with all complaints promptly.**

5. Use and Disclosure

Health information may be used or disclosed by authorised staff for the primary purpose of providing treatment and ongoing care. In addition, it may be used or disclosed for purposes such as health service management, training or research activities; for investigation and law enforcement; in the event of serious and imminent threats to individuals and the public; and in ways that would be reasonably expected for the delivery of patient care.

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 within the health service, to their nominated GP, to another hospital, health service or health professional involved in the patient's care. Advice on how to communicate this information to patients is provided in **Section 7** of this leaflet.

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, to report notifiable diseases, such as cancer and infectious diseases; to report births and deaths; to provide Medicare details.
- For purposes related to the operation of the NSW Health service, for example, to conduct safety and quality improvement initiatives.
- For staff and student training purposes; for planning, financial or management purposes, and for research purposes approved by a Human Research Ethics Committee (in accordance with statutory guidelines issued under privacy law).
- To contact patients regarding patient/client satisfaction surveys that assist to 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 investigate and report a complaint. This includes but is not restricted to complaints about patient care, staff conduct, adverse incidents, patient safety, the health service.
- To comply with a subpoena, summons or search warrant.
- To manage a legal action or claim brought by the patient against the health service.

Further guidance: Privacy Manual, Section 11
Accredited hospital chaplains may use relevant patient information to provide spiritual and pastoral care to patients with a nominated religion. Should patients wish for their religion to be withheld from the chaplaincy service they must advise clinical staff or patient administrative staff.

Further guidance: NSW Health & Civil Chaplaincies Advisory Committee NSW Memorandum of Understanding, PD2011_004

6. Consent

Staff must always obtain consent when it is required, for example, when 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 Medical Record/Clinical Information Department 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 file, or verbally. If provided verbally, this must be clearly documented in the patient file.
Further guidance: Privacy Manual, Sections 5.4 and 11.2.2

7. 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, 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 multi-disciplinary 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. This leaflet is also relevant to staff who are being treated as patients within the health service.
Further guidance: Privacy Manual, Section 7 and Appendix 5

8. Storage and Security

Health information must be stored securely and disposed of appropriately at all times (secure bins or shredding). It should never be put into unlocked bins. It should be protected from unauthorised access, use or disclosure. Medical records and computer screens should not be accessible to unauthorised people.

Unauthorised access includes accessing the electronic medical record (eMR) if you are not involved in the client's/patient's current or ongoing care, or if you are not otherwise authorised to do so.
Further guidance: Privacy Manual, Section 9

9. Access, Amendment and Accuracy

Patients or their authorised representative can apply for access to their medical records (including images). Applications for access or copies of records should be in writing. Some departments may have a procedure in place where sensitive or complex reports or records are accessed with a doctor in the first instance. Staff should check whether this is necessary before granting access.

Staff should make every effort to ensure patient information is accurate. Patients are entitled to request amendment (not deletion) of their health information to ensure it is accurate, up to date and not misleading. If the health service is not willing to make the requested changes, it must **take such steps as are reasonable** to attach additional information to the record. The patient's own comments should be attached as an addendum to the record on request, along with an explanation of the circumstances.
In addition to ensuring correct clinical information, patient information such as name, address, contact person and current GP name must be correct for each encounter.
Further guidance: Privacy Manual, Sections 10 (Accuracy) and 12 (Access and Amendment)

Health
South Eastern Sydney
Local Health District

10. Important Points:

1. All personal information and health information is confidential.
2. Health facilities have an audit capacity in the electronic Medical Record (eMR) and other systems to investigate staff access to patient records. **Staff must only access patient records where this is required for direct patient care or is required in the course of their employment.**
3. Staff should ensure patient privacy is not breached if discussing patient cases and care in public areas, for example; cafeterias, lifts and corridors.
4. Printers and faxes should be located in secure staff areas. Patient information should not accumulate around these.
5. A Health Service may neither confirm nor deny the current or past presence of a person, unless the enquirer already knows that the client/patient is present. No personal health information, including admission and discharge dates, should be given over the telephone unless it has been established that the caller has legitimate grounds to access the information and can give proof of identity. If there are concerns regarding the legitimacy of the call, the matter should be escalated to the Senior Nurse Manger.
6. Staff should not disclose patient information without delegated authority, authorisation from a manager or without patient consent.
7. Fees and charges may be raised for provision of copies of medical records.
8. Database managers and custodians must ensure compliance with all privacy principles. Records containing information pertaining to Adoption, Organ/Tissue Donor, Child Protection, Sexual Assault, Genetic Information, Drug & Alcohol and sexual health have additional restrictions on use and disclosure.
9. Staff can confirm the identity and address of a patient with police. Staff should obtain the police officer's name, badge number and phone number before releasing patient information.

Further guidance: Privacy Manual Section 15.9.

SESLHD Medical Record Managers – Located in Medical Records Departments at each site.

Calvary Hospital: Jennifer O'Hearn 9553 3591
Randwick Campus (POW/SCH/RHW): Sophia Adamo 9382 3706
St George Hospital: Vivienne Rowlands 9113 2087
Sutherland Hospital: Rachel Kelloway 9540 7154
Sydney/Sydney Eye Hospital: Lyudmila Nikolenko 9382 7338
War Memorial Hospital: Robyn Counter 9369 0242

Reference materials available at: http://internal.health.nsw.gov.au/privacy/resources.html
NSW Health Privacy Manual, PD2005_593
NSW Internal Review Guidelines, GL2006_007
NSW Privacy Management Plan, PD2005_554
NSW Health & Civil Chaplaincies Advisory Committee NSW Memorandum of Understanding, PD2011_004
NSW Health Privacy Leaflet for Patients