PRIVACY MANUAL
FOR HEALTH INFORMATION

NSW GOVERNMENT Health

NSW MINISTRY OF HEALTH
73 Miller Street
NORTH SYDNEY NSW 2060
Tel. (02) 9391 9000
Fax. (02) 9391 9101
TTY. (02) 9391 9900
www.health.nsw.gov.au

SHPN (LRS) 150001
ISBN 978-1-76000-002-8

Further copies of this document can be downloaded from the NSW Health website www.health.nsw.gov.au

March 2015

Contents

NSW Health Privacy Manual for Health Information
Record of Amendment

No.	Approval Date	Reason for amendment	Pages removed	Pages inserted

No.	Approval Date	Reason for amendment	Pages removed	Pages inserted

1 Definitions and acronyms

Note: Terms frequently used in this document are defined below. Please note they are intended for use and interpretation within the context of this document only.

Accredited chaplain – A person accredited in accordance with the *NSW Health & Civil Chaplaincies Advisory Committee NSW Memorandum of Understanding (MOU)*, to provide pastoral care and chaplaincy services to patients. See **Section 11.2.10** Chaplaincy services.

Affiliated health organisation – An organisation or institution listed in Schedule 3 of the *Health Services Act 1997*. See **Section 3.1 Who is bound by the Manual?**

Ambulance Service of NSW – A health service of the NSW public health system. See also **'Health service'** and **'Public health system'**.

Authorised representative – See **Section 5.6 Authorised representative**

Capacity – See **Section 5.5 Test for capacity**

Chief Executive – Under the *Health Services Act 1997,* Chief Executive means the Chief Executive of a Local Health District, Specialty Network or statutory health corporation, or the person responsible to the governing body of an affiliated health organisation for management of its recognised establishments and services.

Child – a person who is under the age of 16 years, as defined in the *Children and Young Persons (Care and Protection) Act 1998*, section 3. See also '**Young person**' and '**Minor'**.

Confidentiality – For the purposes of this Manual, confidentiality is a professional duty or a promise between a health practitioner and his or her patient that places restrictions on the disclosure of information provided by the patient as part of the care and treatment given by the practitioner. The duty of confidentiality is not absolute, and there are circumstances where a practitioner may lawfully disclose the patient's information. See **Section 4.3.1 Duties of confidentiality.**

Consent – Permission for something to happen or agreement to do something. See **Section 5.4 Consent.**

Data – A representation of facts, concepts or instructions in a formalised manner suitable for communication, interpretation or processing by human beings or by automatic means.

De-identified data – De-identified data or information is information or opinion about a person whose identity cannot be ascertained from the information or opinion. See **Section 5.3 De-identified information.**

'Directly related purpose' – A health service may use or disclose personal health information if it is a purpose *directly related* to the primary purpose, **and** the individual would reasonably expect the health service to use the information for this purpose. See **Section 11.2.1 Directly related purpose.**

Enduring power of attorney – A formal document which authorises another person to make financial and legal decisions where the patient is unable to make these decisions for themselves. See also **'power of attorney'**, and **Section 5.6 Authorised representative.**

Enduring guardian – A formal document which authorises another person to make health and lifestyle decisions on the patient's behalf, including the authority to consent to medical and dental treatment. See **Section 5.6 Authorised representative.**

FACS – The NSW Department of Family and Community Services

Genetic relative – means a person who is related to an individual by blood, for example, a sibling, parent or descendant of the individual.

GIPAA – The *Government Information (Public Access) Act 2009*

GP – means 'general practitioner'. A general practitioner (or GP) is a registered medical practitioner who is qualified and competent for general practice.

Health information – see **Section 5.1 Health information**.

Health Information Service – refers to the unit, department or service within a health service responsible for managing personal health information and patient health records. This includes responsibility for the development and maintenance of health information systems.

Note: Health Information Service holds the same meaning as: 'Health Information Unit, 'Medical Record Department', 'Health Information and Record Service', 'Clinical Information Department', and so on.

Health practitioner – Anyone, including a medical practitioner, who is a registered health professional under the Health Practitioner Regulation National Law.

Health record – A documented account, whether in hard copy or electronic form, of a patient's health, illness and treatment during each visit or stay at a health service.

Note: Health record holds the same meaning as: 'health care record', 'medical record', 'clinical record', 'clinical notes', 'patient record', 'patient notes', 'patient file', and so on.

Health (or medical) research – Systematic investigation undertaken for the purpose of adding to the body of knowledge pertaining to human health.

Health service – A public health organisation (including a Local Health District or Specialty Network), a statutory health corporation, the Ambulance Service of New South Wales, and Units of the Health Administration Corporation. See **Section 3.1 Who is bound by the Manual?**

Health service staff – Anyone who carries out work for a NSW health service, including employees, visiting health practitioners, contractors and sub-contractors, agency staff, volunteers, apprentices, trainees, and students. See **Section 3.1 Who is bound by the Manual?**

Hospital – means a hospital as defined in Part 1 of the *Health Services Act 1997*, being an institution at which relief is given to sick or injured people through the provision of care or treatment.

HPPs – The Health Privacy Principles established under the *Health Records and Information Privacy Act 2002*. There are 15 HPPs. See **Section 2.1 Overview of privacy legislation**.

HREC – Human Research Ethics Committee a committee, constituted in accordance with NHMRC guidelines, which protects the subjects of research and ensures that ethical standards are maintained by reviewing and advising on the ethical acceptability of research proposals.

HRIP Act – the *Health Records and Information Privacy Act 2002 (NSW)*.

HRIP Regulation – the *Health Records and Information Privacy Regulation 2012 (NSW).* See **Section 3.2 NSW Health agencies to be treated as a single agency**.

Immediate family member – Defined under section 4 of the *HRIP Act* to be a person who is:

- a parent, child or sibling of the individual, or
- a spouse of the individual, including a de facto spouse, 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.

Local Health District (LHD) – A health service constituted under the *Health Services Act 1997*, Schedule 1.

Medical practitioner – a registered health professional under the Health Practitioner Regulation National Law.

Medical record – see health record.

Ministry of Health – The NSW Ministry of Health as established under the *Public Sector Employment and Management Act 2002*.

Minor – A minor is a person under the age of 18 years old. See also **'Child'** and **'Young person'**.

NHMRC – National Health & Medical Research Council.

NSW Health – a term defined in the *Health Administration Act 1982*, section 4 (1A) which describes any body or organisation under the control and direction of the Minister for Health or the Secretary, NSW Health.

NSW PHSREC – NSW Population and Health Services Research Ethics Committee – the NSW Health Human Research Ethics Committee established in accordance with NHMRC guidelines.

Parental responsibility – Defined in section 8 of the *HRIP Act* to be all the duties, powers, responsibility and authority which, by law, parents have in relation to their children.

Patient – Any person who receives a health service and to whom, as a result, a health practitioner owes a duty of care. For the purposes of this Manual, the term 'patient' has been chosen to represent both clients and patients of a NSW health service, for ease of use.

PCEHR – The **Personally Controlled Electronic Health Record**, or National eHealth Record, is operated by the Commonwealth Government Department of Health and enables patients to view a summary of their health records online. See **Section 16.8 National eHealth Record**.

PCO – Privacy Contact Officer – see **Section 6.2 Privacy Contact Officer**.

Personal health information – see **Section 5.1 Health information**.

Personal information – see **Section 5.2 Personal information**.

PPIP Act – The *Privacy and Personal Information Protection Act 1998 (NSW).*

Power of attorney – A formal document in which a person of sound mind authorises a second person to act on their behalf. See also **'Enduring power of attorney'**, and **Section 5.6 Authorised representative**

'Primary purpose' – the "dominant purpose" for which personal health information is collected. Most often in the health system, the collecting purpose will be to provide care, or an episode of care.

Privacy – for the purposes of this Manual, 'privacy' refers to the right of an individual to have their personal health information safeguarded from loss, misuse and unauthorised disclosure in order to protect the privacy of an individual's personal health information. See also **Section 2.1 Overview of privacy legislation**.

Public health organisation – Under the *Health Services Act 1997*, a public health organisation is a Local Health District or a statutory health corporation (including Specialty Health Networks), or an affiliated health organisation in respect of its recognised establishments and services.

Public health system – All public health organisations in NSW, the NSW Ministry of Health, the Ambulance Service of NSW, and all other organisations under the control and direction of the NSW Minister for Health or the Secretary of NSW Health. See **Section 3.1 Who is bound by the Manual?**

Record keeper – The person who has administrative control of a health record, a Health Information Manager.

Secondary purpose – The health service may use or disclose personal health information for a "secondary purpose" in accordance with Health Privacy Principles 10 and 11. See **Section 11.2 Use and disclosure for a "secondary purpose".**

Security – A tangible set of physical and logical mechanisms which can be used to protect information held in hard and soft copy, digital format, within computer systems, via telecommunications infrastructure, etc.

Specialty Network – Sydney Children's Hospitals Network and Justice & Forensic Mental Health Network.

Staff – see **'Health service staff'**.

Statutory guidelines – Refers to guidelines under the *HRIP Act* issued by the NSW Privacy Commissioner, Information and Privacy Commission NSW. See **Section 11.2.4 Management, training or research**.

Statutory health corporation – A corporation, listed in Schedule 2 of the *Health Services Act 1997*, which provides certain health support services other than on an area basis (including The Justice and Forensic Mental Health Network, The Sydney Children's Hospitals Network).

Use of personal health information – Refers to the communication or handling of information within NSW Health. There are three broad categories of use, those being where information is used for the "primary purpose" for which it is collected, where information is used for another "secondary purpose" and one of the criteria listed in the HPPs applies, or where the use of the information is lawfully authorised. See **Section 11 Using & disclosing personal health information (HPPs 10 & 11)**.

Young person – a young person means a person who is aged 16 years or above but who is under the age of 18 years, *Children and Young Persons (Care and Protection) Act 1998*, section 3. See also '**Child'** and **'Minor'**.

2 Executive Summary

This is the third edition of the NSW Health Privacy Manual, now titled NSW Health Privacy Manual for Health Information. (The previous 2 editions have been titled NSW Health Privacy Manual.) This edition has incorporated changes in legislation which impact on the management of personal health information within NSW Health, notably:

- the *Public Health Act 2010*
- the *Mental Health Act 2007*
- the *Work Health and Safety Act 2011*
- Chapter 9A, the *Coroners Act 2009* (Domestic Violence Death Review Team)
- changes to the *Children and Young Persons (Care and Protection) Act 1998*
- introduction of the *Government Information (Public Access) Act 2009*

The NSW Health Privacy Manual for Health Information provides operational guidance to the legislative obligations imposed by the *Health Records and Information Privacy Act 2002*. The manual outlines procedures to support compliance with the Act in any activity that involves personal health information.

Consultation on this third edition has extended to:

- the Ministry of Health
- Local Health Districts (LHDs), Specialty Networks and public health organisations (PHOs) comprising NSW Health
- the NSW Privacy Commissioner, Information and Privacy Commission NSW

2.1 Overview of privacy legislation

As noted in the first edition, privacy in Australia has moved from a policy based system to one regulated by law. In NSW, these laws are the *Health Records and Information Privacy Act 2002 (HRIP Act)* which regulates health privacy, and the *Privacy and Personal Information Protection Act 1998 (PPIP Act)* which applies to non-health personal information. As privacy policy is set by legislation, the role of this Manual is to provide operational guidance to assist in compliance with the *HRIP Act*.

The Manual provides a guide to the legislative obligations imposed on the health system by the *HRIP Act* and outlines procedures to support compliance with the Act in activities that involves personal health information. Specific purposes include:

- ensuring personal health information is collected, stored and used in accordance with the HRIP Act
- providing health service staff with assistance and practical tips for complying with the HRIP Act
- acknowledging the responsibility of the NSW public health system to ensure that the privacy of patient information is protected
- meeting the need of health service staff for clear guidance on what is acceptable and what is not when dealing with personal health information in order to remove pressure and uncertainty from those who are involved in the day to day administration of such information
- constituting a benchmark which can be used for auditing performance.

The Health Privacy Principles (or HPPs) contained in the *HRIP Act* establish 15 rules for the management of information. Some of these rules will mainly be relevant when setting up data collections or patient information systems, such as:

- Collection Principles (HPPs 1-3)
- Retention and Security (HPP 5)
- Identifiers (HPP 12)
- Linkage of Electronic Records (HPP 15)

Other HPPs will be relevant to how you interact with patients and meet their information needs:

- Collection Principle (HPP 4)
- Access (HPPs 6-7)
- Amendment (HPP 8)
- Anonymity (HPP 13)

Others will also be important in the day to day use of personal health information in the NSW public health system, and deciding when and how to share that information:

- Accuracy (HPP 9)
- Use (HPP 10)
- Disclosure (HPP 11)
- Transfer of Information Across State Borders (HPP 14)

While the HPPs are applicable across the board, they will be particularly relevant if involved in the above activities. In these cases, you should look particularly closely at the issues raised in the Manual.

2.2 Summary of the Health Privacy Principles (or HPPs)

The 15 Health Privacy Principles (or HPPs) are set out in the *Health Records and Information Privacy Act 2002*, Schedule 1, available via the NSW Government legislation website at:
www.legislation.nsw.gov.au/

The HPPs are summarised below for quick reference.

COLLECTION PRINCIPLES	
HPP 1	**Purposes of collection of personal health information**
Personal health information must be collected by lawful means and for a lawful purpose. The purpose must be directly related to, and reasonably necessary for, an organisation's functions or activities.	
HPP 2	**Collection and information sought must be relevant, not excessive, accurate and not intrusive**
HPP 3	**Collection from individual concerned**
Personal health information must be collected from the individual it relates to, unless that is unreasonable or impractical.	
HPP 4	**Individual to be made aware of certain matters**
Reasonable steps must be taken to inform the individual about how the information may be used, who may access it, and the consequences of not providing it. The individual should be told what agency is collecting the information and that they have a right to access it. This information should generally also be given to the individual where information about them is collected from someone else, unless certain exemptions, listed in the Act and the guidelines apply.	
SECURITY PRINCIPLES	
HPP 5	**Retention and security**
Personal health information held by public health agencies must be securely housed and protected against loss or misuse. Information must be kept only as long as is necessary for the purpose (or as required by a law, such as the *NSW State Records Act 1998*), and must be disposed of securely.	

ACCESS AND AMENDMENT PRINCIPLES	
HPP 6	**Information about personal health information held by organisations**

Organisations that hold personal health information must allow individuals to find out if they hold information about that individual, and, if so, what kind of information they hold, what it is used for, and whether and how the individual can access it.

HPP 7	**Access to personal health information**

Individuals must be allowed to access the personal health information held about them. This must be done without excessive expense or delay.

HPP 8	**Amendment of personal health information**

Individuals may request that their personal health information be amended to ensure that it is accurate, relevant, up to date, complete and not misleading.

Organisations must either make the requested amendments or, if requested, attach to the information a statement by the individual of the amendment they sought.

ACCURACY PRINCIPLES	
HPP 9	**Accuracy**

Before using personal health information, organisations must take reasonable steps to ensure that the personal health information they hold is relevant, up to date, complete and not misleading.

USE PRINCIPLES	
HPP 10	**Limits on use of personal health information**

Personal health information can be used for the purpose for which it was collected, or for other purposes recognised by the Act. These include a "secondary purpose" such as where there is consent for the use, the use is a "directly related purpose", for management, training and research activities, for investigation and law enforcement, or where there are serious threats to individuals or the public.

DISCLOSURE PRINCIPLES	
HPP 11	**Limits on disclosure of personal health information**

The provisions for disclosure of personal health information are the same as those for use of this information. They also include a provision that a person's personal health information may be disclosed to immediate family members for compassionate reasons, provided that this is not contrary to the expressed wish of the individual.

OTHER PRINCIPLES	
HPP 12	**Identifiers**

Identifiers can only be applied to personal health information if this is reasonably necessary to carry out the organisation's functions. Public health system identifiers may be used by private sector agencies, but only in defined circumstances and with strict controls.

HPP 13	**Anonymity**

Provided that it is lawful and practicable, individuals should be given the option of not identifying themselves when dealing with health organisations.

HPP 14	**Transborder data flows and data flows to Commonwealth agencies**

As a general principle, personal health information must not be transferred to a Commonwealth agency or an organisation in another state jurisdiction unless the receiving agency applies personal health information privacy policies and procedures substantially similar to those of NSW.

HPP 15	**Linkage of health records**

Personal health information must not be included in a system outside NSW Health that links health records of one health service with health records in another health service, unless the individual it relates to has expressly consented. HPP 15 only applies to linkages of an ongoing record of health care for an individual and does not restrict linkage of other personal health information held electronically.

HPP 15 will apply to the linkage of records of health care at a state or national level between the public and private sectors, or between two or more private health services.

Further guidance: Section 13.3 Linkage of health records (HPP 15) – Section 16.8 National eHealth Record

2.3 Quick reference to structure of the Manual

For a general overview of the rationale and purposes for this Manual	Go to Section 2.1
For a summary of the Heath Privacy Principles (HPPs) under the *HRIP Act*	Go to Section 2.2
For explanation of how other laws relate to privacy law	Go to Section 4
To check the meaning of some of the "key concepts" used in privacy law	Go to Section 5
For a detailed explanation of the HPPs	Go to Sections 7-13
If you have received a complaint, or need to conduct an internal review	Go to Section 14
If you need to check how to deal with common privacy issues arising in health care	Go to Section 15
For: ■ List of relevant NSW Health policies ■ List of relevant laws ■ Pro forma privacy undertaking ■ Pro forma privacy notices ■ Pro forma patient leaflet ■ Pro forma staff information sheet ■ Consent guide for medico-legal requests	 Go to Appendix 1 Go to Appendix 2 Go to Appendix 3 Go to Appendix 4 Go to Appendix 5 Go to Appendix 6 Go to Appendix 7

If you have any feedback on the Manual, it should be sent to:
Legal and Regulatory Services
NSW Ministry of Health
LMB 961 NORTH SYDNEY NSW 2059
E-mail: LegalMail@doh.health.nsw.gov.au

3 Scope

3.1 Who is bound by the Manual?

The Manual applies to all people who work within the NSW public health system. These include, but are not limited to, staff members, contractors and other health care providers who, in the course of their work, have access to personal health information.

The Manual applies to people whose employment is full time, part time, permanent, temporary, casual, contractual, or short term. These include, but are not limited to, volunteers and people who do unpaid work either as community volunteers, clinical students, and clinicians working or observing as research fellows.

Persons to whom the Manual applies include:

- providers of health services such as doctors, nurses, midwives, case managers, visiting providers and allied health staff
- administrators, clerical and service staff
- technical, scientific and laboratory personnel
- auditors
- interpreters
- accredited chaplains
- pastoral care workers
- volunteers
- students
- consultants
- temporary and contract staff
- external custodians of information owned by the NSW Ministry of Health.

The Manual applies to NSW Health, which covers:

- Local Health Districts (LHDs)
- Statutory Health Corporations
- Specialty Networks
- Affiliated health organisations
- Units of the Health Administration Corporation, including the Ambulance Service of NSW
- the NSW Ministry of Health
- the Cancer Institute NSW
- any other health service provided by the public health system including nursing homes, hostels and group homes, community health services, drug and alcohol services, allied health programs, dental and early childhood services, multi-purpose services, scientific and laboratory services and health promotion and public health services
- non-government organisations receiving funding from the Ministry where compliance is included in the terms of their Funding Agreement
- staff of the Health Professional Councils Authority employed by the Health Administration Corporation

Further guidance

- Corporate Governance & Accountability Compendium for NSW Health
- Privacy Information Leaflet for Staff (See Appendix 6)

3.2 NSW Health agencies to be treated as a single agency

In accordance with clause 7 of the *Health Records and Information Privacy Regulation 2012, certain public sector agencies to be treated as a single agency*, the following health agencies are to be treated as a single agency for the purposes of the Health Privacy Principles:

(a) the NSW Ministry of Health
(b) the Health Administration Corporation
(c) local health districts
(d) statutory health corporations (including Specialty Networks)
(e) the Cancer Institute (NSW)

This Regulation enables multiple NSW Health agencies to provide health services to an individual within the scope of the 15 Health Privacy Principles. Prior to the Regulation, it was possible that normal processes for the collection, storage, use and disclosure of personal health information between NSW Health agencies may have constituted a breach of the *HRIP Act*.

Use of personal health information between these agencies must still comply with the requirements of HPP 10 (Limits on use).

Further guidance

- Section 11 Using & disclosing personal health information (HPPs 10 & 11)

3.3 What sort of information does the Manual cover?

The Manual covers personal health information. Under the *HRIP Act* this means personal information that is identifying information, or which could reasonably link to identifying information, collected from or about individual people in order to provide them with health services. See Sections 5.1 Health information, and 5.2 Personal information.

Both the *HRIP Act* and the Manual cover all types of dealings with personal health information, including collection, storage, security, use, disclosure, access, transfer and linkage of health records. They apply to personal health information in any format, including electronic and online formats as well as paper-based health records. While different formats will require different approaches and procedures, the underlying principles remain the same.

3.4 What is not covered?

The *HRIP Act* and the Manual do NOT apply to:

- information that is not "personal information" but which may be considered sensitive such as tender documents, private hospital licensing information or Cabinet documents
- information that is not personal information as it is "de-identified" or because the identity of a person is not reasonably ascertainable from the information
- personal information which is not health information, such as payroll records or personnel files (these are regulated by the *PPIP Act*)
- statistical or other aggregated information

Further guidance

- PD2005_554: Privacy Management Plan
- PD2012_018: Code of Conduct
- PD2014_005: Goods and Services Procurement Policy
- NSW Public Service Personnel Handbook

3.5 What our patients have a right to expect

Patients should be informed that:

- their personal health information will be protected in accordance with the *HRIP Act*
- their personal health information will be given to another person only if this is important for their health care or can be otherwise legally and ethically justified
- they are, subject to limited exceptions, entitled to access their own health records and have those records amended to correct inaccuracies
- provided it is both legal and practicable to do so, they will have the opportunity to obtain services anonymously (see Section 8 Anonymity (HPP 13))
- comprehensive clinical information will be available to their health care providers to enable optimal care.

Further guidance

- Section 7 – Collecting personal health information (HPPs 1-4)

3.6 What health staff and service providers have a right to expect

NSW Health is committed to ensuring that information which supports the provision of health care is readily available to authorised users, when and where it is needed and is delivered in a timely and efficient manner. Accordingly, the Manual supports the principles in the *HRIP Act* which also promote:

- **the integrity of data**, so that information is accurate, complete and up-to-date. Information integrity is critical for quality patient care, evaluation of services, medical research and the maintenance of public health.
- **access to personal health information for authorised persons** for legitimate health purposes. It is recognised that if appropriate information is not readily available to providers of health services, the care or interests of patients may be compromised.
- **the optimum use of data**, primarily for the benefit of those patients to whom the data relates but also for the general betterment of the health of the population of New South Wales through public health surveillance and medical research.

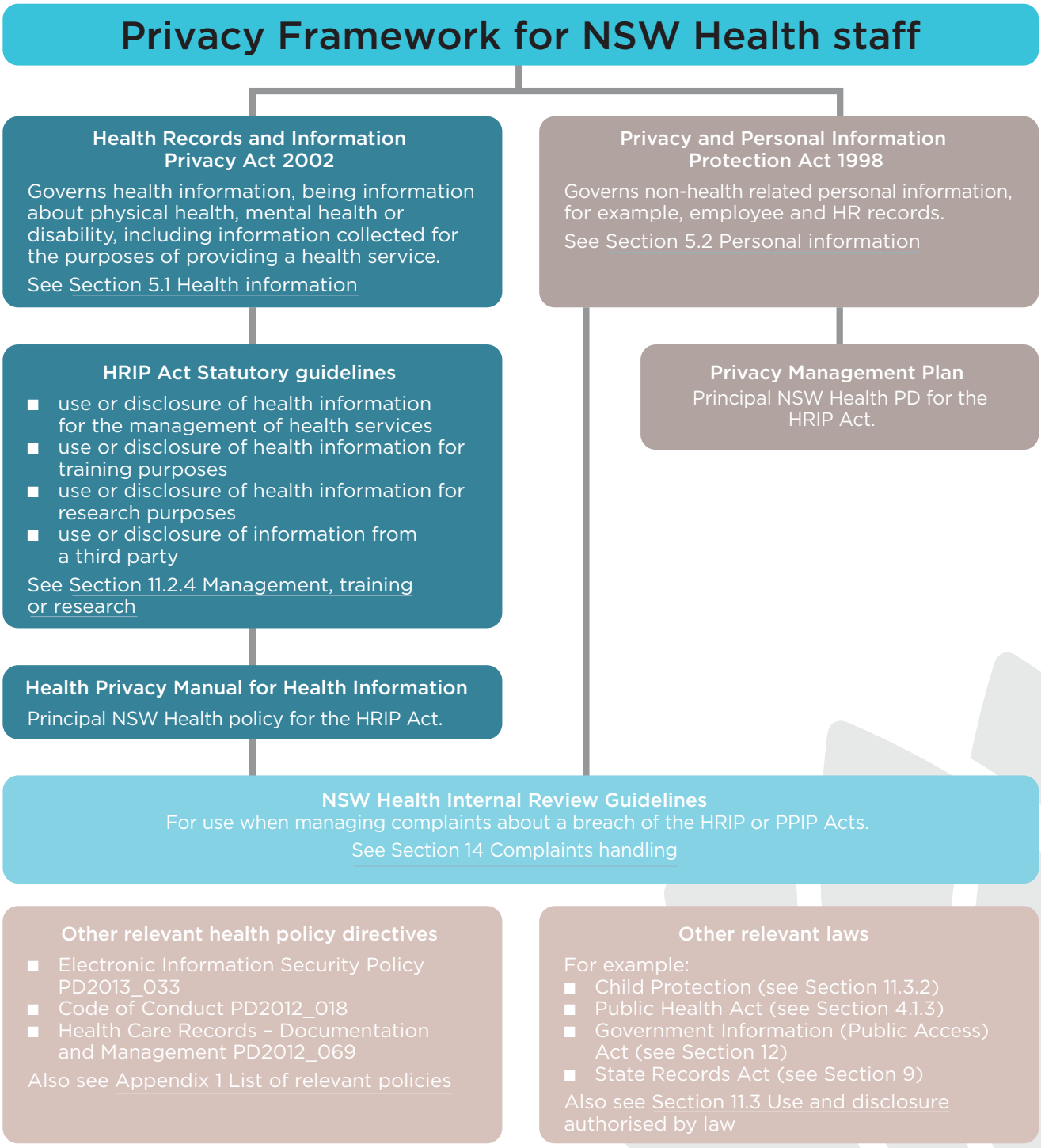
3.7 What other NSW Health resources should be considered

This Manual provides a broad overview of the key privacy obligations established under the *HRIP Act*. There are however a range of other NSW Health policies which are also relevant to the collection, use, storage and disclosure of information in NSW Health.

The main policies are referenced in the body of the Manual. In addition, a comprehensive list of related NSW Health policies is set out in Appendix 1. The Manual should be read in conjunction with these policies.

3.8 Privacy Framework for NSW Health staff

To assist staff identify which privacy legislation applies to their circumstances or to a particular issue at hand and where to go for *further guidance*, refer to the privacy framework below:



4 Other obligations

4.1 Privacy laws and related legislation

Privacy obligations in NSW generally arise from two separate laws.

- the *Privacy and Personal Information Protection Act 1998 (NSW)*, which regulates personal information in the public sector in NSW
- the *Health Records and Information Privacy (HRIP) Act 2002 (NSW),* which regulates personal health information in the public and private sectors in NSW.

The health system relies upon the Health Privacy Principles contained within the *Health Records and Information Privacy Act 2002*, or *HRIP Act*, to use and disclose personal health information. See Section 2.2 Summary of the Health Privacy Principles (or HPPs).

There are, however, other pieces of legislation which impose specific controls on when and how information can be used and disclosed, or allow for use and disclosure of information in circumstances which the Health Privacy Principles would not otherwise allow. The most important of these are:

4.1.1 *Health Administration Act 1982*

The *Health Administration Act* covers any information which is provided or recorded pursuant to any Act in the health portfolio. It is binding on all persons working in the NSW Health system. Under section 22 of the Act information cannot be disclosed unless certain specified criteria are satisfied. These criteria cover:

- where the person to whom the information relates consents to the release
- where the release occurs in connection with the administration of health legislation (i.e. where other legislation such as the *Public Health Act* authorises or requires disclosure)
- where the release is for the purposes of legal proceedings arising out of health legislation, e.g. pursuant to a court order or subpoena
- when there is an 'other lawful excuse' such as, orders under other court proceedings, assisting the police in investigating a specific criminal offence, or a lawful direction by the Minister or Secretary, NSW Health
- in circumstances set out in Regulations under the Act.

The *Health Administration Regulation 2010* currently exists to allow the Chief Health Officer to release epidemiological data and the Secretary, NSW Health to release other information for the purposes of research. Such data are only released to bona fide researchers and on condition that the confidentiality of data is maintained.

Clause 16 of the Regulation, allows these disclosures if:

- the information is epidemiological data and
- the disclosure is made in accordance with the written approval of the Chief Health Officer and
- that approval describes the information that is authorised to be disclosed and names the person or body to whom disclosure is authorised.

Clause 14 of the Regulation also allows disclosure of information in certain circumstances where it is necessary for Root Cause Analysis (RCA) related matters. The Act provides for a penalty of a fine of up to 10 penalty units or imprisonment for a term not exceeding 6 months.

4.1.2 *Mental Health Act 2007*

The *Mental Health Act* governs the way in which the care and treatment of people in NSW is provided to those people who experience a mental illness or mental disorder.

The Act limits the release of personal health information unless certain criteria, similar to those set out above in 4.1.1, are met, or in accordance with HPP 10(1) and HPP 11(1). It is of particular relevance to people working in the mental health field. The Act provides for a penalty of a fine of up to 50 penalty units for unauthorised disclosure of information.

Primary carers

Division 2 of Chapter 4, Part 1 of the Act deals with information sharing. This division deals with sharing information with the patient, their carer or representative at a Mental Health inquiry or before the Tribunal relating to medication, mental health inquiries, detention, movements, reclassification and discharge of patients. There are also specific provisions giving primary carers rights to certain information, particularly in relation to notification of detention, and discharge planning.

Mental Health Emergency Response

Reference should be made to the Mental Health Emergency Response 2007:

Memorandum of Understanding (MOU) between NSW Health including the Ambulance Service of NSW, and NSW Police Force.

The MOU provides for the collaborative management of persons who have a mental illness or mental disorder, or who exhibit behaviours of community concern.

Chapter 7.2 Privacy and Information Exchange of the MOU provides guidance on the circumstances when personal health information can be shared with the NSW Police Force, and examples of the types of relevant information that may be shared.

The Mental Health Emergency Response 2007: Memorandum of Understanding is available as a NSW Health publication at: www0.health.nsw.gov.au/pubs/2007/mou_mentalhealth.html

Further guidance

- IB2010_044: Mental Health Information and the Health Records and Information Privacy Act 2002
- *Mental Health Act 2007* Guidebook
- *Mental Health Act 2007* Information Sheet for Consumers and Carers

Publications of NSW Health and the Institute of Psychiatry are available at:

- www.health.nsw.gov.au/mhdao
- www.nswiop.nsw.edu.au

4.1.3 *Public Health Act 2010*

Section 130 of the *Public Health Act* prevents release of personal health information unless certain criteria are met.

A person who discloses any information obtained in connection with the administration or execution of this Act is guilty of an offence unless the disclosure is made:

(a) with the consent of the person from whom the information was obtained, or

(b) in connection with the administration or execution of this Act or the regulations, or

(c) for the purposes of any legal proceedings arising out of this Act or the regulations, or of any report of any such proceedings, or

(d) with the approval of the Chief Health Officer, or a person authorised by the Chief Health Officer to give the approval, to a person specified in the approval and the information consists of epidemiological data specified in the approval, or

(e) in other prescribed circumstances (i.e. where provided for in regulations under the *Public Health Act*), or

(f) with other lawful excuse (i.e. where there are other statutory obligations to disclose).

The Act provides for a penalty of a fine of up to 100 penalty units or imprisonment for 6 months, or both for a breach of section 130.

4.1.3.1 Epidemiological data

Both the *Health Administration Regulation 2010 (clause 16)* and the *Public Health Act 2010 (section 130)* allow for the release of epidemiological data where there is written approval from the Chief Health Officer.

Further guidance

- *PD2012_051: Data Collections – Disclosure of Unit Record Data held for Research or Management of Health Services.*
- Section 15.14 – NSW data collections

4.1.3.2 HIV/AIDS-related information

The most important confidentiality provision in the *Public Health Act* deals specifically with 'HIV/AIDS-related information'.

Under the Act this means two things:

- the fact that a person has had or is going to have an HIV test, or
- the fact that a person is HIV positive or has AIDS.

Section 56 of the Act places strict limitations on the release of this information.

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 so long as the information is relevant to the provision of such care, treatment or counselling, 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*, or
- in the circumstances prescribed by the regulations.

The Act provides for a penalty of a fine of up to 100 penalty units or imprisonment for 6 months, or both for a breach of section 56.

Further guidance

- Section 11.2.3.3 – *Public Health Act 2010* – Notification of public health risk
- Section 15.9.6 – Managing public health risks

4.1.4 *Privacy Act 1988 (Commonwealth)*

This Act and the *Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Commonwealth)* do NOT apply to the NSW public sector.

The Commonwealth privacy legislation is limited to the regulation of the Commonwealth public sector and the private sector in NSW including non-government organisations. Its provisions relating to health information do not therefore apply to NSW Health and should not be relied on.

NSW Health agencies however should be aware that Commonwealth privacy legislation may bind non-government organisations and private sector health providers (such as individual health practitioners and private hospitals), and so may be relevant to the way these organisations interact with NSW Health.

For example, if a Commonwealth agency engaging in a data sharing arrangement with a NSW Health agency has specific requirements regarding the management of personal health information held by the Commonwealth agency, they should identify the specific Australian Privacy Principle(s) and advise NSW Health of any additional protections required. In general, the NSW privacy legislation is largely consistent with the Commonwealth privacy legislation, and therefore it is not anticipated that there will be any barriers within the separate pieces of legislation for data-sharing arrangements to be developed.

Health services should always be mindful that disclosures to Commonwealth agencies, as with all other agencies, meet the standard limits for disclosure under the *HRIP Act*.

Further guidance

- Section 11 Using & disclosing personal health information (HPPs 10 & 11)
- Section 13.2 Transferring personal health information outside of NSW (HPP 14)

4.1.5 *Children and Young Persons (Care and Protection) Act 1998*

Chapter 16A of the *Children and Young Persons (Care and Protection) Act* facilitates the exchange of information between prescribed agencies for the safety, welfare and wellbeing of a child or young person. Exchange of information in accordance with Chapter 16A does not constitute a breach of privacy laws.

Further guidance

- *Section 11.3.2 Child protection*

4.2 Other laws regulating information management

4.2.1 *State Records Act 1998*

The *State Records Act* provides for the creation, management and protection of the records of public offices of the State, and for public access to those records.

The Act overlaps with the *HRIP Act* in relation to the retention and disposal of records held by public sector agencies, and public access to those records.

The Act is not affected by the *HRIP Act*, which means that public sector agencies must comply with the requirements of both Acts.

Further guidance

- Section 9.1 Retention and disposal of personal health information

4.2.2 *Government Information (Public Access) Act 2009*

The *Government Information (Public Access) (GIPA) Act 2009* replaces the *Freedom of Information Act 1989*. The *GIPA Act* allows *any* person to apply for access to *any* information held by government. It is different from the *HRIP Act* as it is designed to facilitate open and transparent government and is not restricted to personal

information, whereas privacy laws are designed to provide individuals with greater knowledge and control over their own information.

As a general principle, health services should rely on the access provisions in privacy law rather than the *GIPA Act*, and integrate its principles into their day to day work. The *GIPA Act* should however still be used where:

- The patient (or their legal representative) declines access under the *HRIP Act* and specifically requests access under the *GIPA Act*. Their application should be processed, and should not be refused simply because they choose not to use the *HRIP Act*.
- The information sought relates to a number of people or is sought in the context of a family dispute or raises other contentious issues. The *GIPA Act* provides a structured process for consultation with people other than the applicant who may be affected by release of information. It will therefore be a useful alternative in such cases.
- Where a family seeks information about a relative who is deceased, and there is no appropriate "authorised representative" to consent to the disclosure.

Further guidance

- *Section 12 Patient access and amendment (HPPs 6, 7 & 8)*

4.3 Common law and professional obligations

4.3.1 Duties of confidentiality

Health care providers also owe patients a common law duty of confidentiality in relation to information obtained as part of the treating relationship. The duty is based in part on contract law and also on the "fiduciary duty" of an individual practitioner to his or her patients. The duty is not absolute and there are circumstances where a provider may lawfully disclose the information. These situations include where the patient waives their right to confidentiality, or where there is some statutory or other lawful excuse – such as for example, a court order or subpoena, or statutory provisions for mandatory notification (as occurs in relation to suspected child abuse, and certain notifiable diseases), and mandatory notification obligations imposed on registered practitioners. Health care providers should consider their common law duties when considering release of information.

The common law also allows a disclosure to be made "in the public interest" where the disclosure is necessary to prevent a serious risk of harm. This recognises that there will be circumstances where the public benefit of the information being disclosed is sufficient to outweigh the public interest in maintaining confidentiality. The exact nature and extent of this interest, and when it will apply, remains somewhat uncertain, but is likely to be similar to Health Privacy Principle 11(1)(c) where disclosure is permitted where there is a serious and imminent threat to the life, health or safety of an individual, or a serious threat to public health or public safety (see Section 11.2.3 To prevent a serious and imminent threat to health or welfare).

4.3.2 Registered health professionals

Some health professional groups are registered under the *Health Practitioner Regulation National Law (NSW)*. This health professional registration legislation provides a basis for clinical and professional standards based on definitions of 'unsatisfactory professional conduct' and 'professional misconduct'. Breach of the confidence owed by a health practitioner to a patient may constitute professional misconduct and may therefore be subject to disciplinary action.

Various professional codes of ethics also require that confidentiality of personal information be maintained. Although such codes do not have the binding authority of a statute, breaches may incur disciplinary action for registered health practitioners under the National Law. More broadly, they are a reflection of the prevailing view of proper conduct among the health professions.

4.4 NSW Health Code of Conduct

The NSW Health Code of Conduct defines standards of ethical and professional conduct that are required of everyone working in NSW Health. Chief Executives are responsible for ensuring that the Code is promulgated throughout their agency.

The Code of Conduct promotes a standard of behaviour which demonstrates respect for the rights of the individual and the community and maintains public confidence and trust in the work of the public health system. Section 4.5 of the Code of Conduct includes requirements for observing the privacy, confidentiality and security of information obtained during the course of employment within NSW Health, as shown below.

Further guidance:

- PD2012_018: NSW Health Code of Conduct

NSW Health Code of Conduct (PD2012_018)

4.5 Maintain the security of confidential and/or sensitive official information.

Staff must:

4.5.1 keep confidential all personal information and records

4.5.2 not use or release official information without proper authority, such as discussing or providing information on social media that could identify patients or divulge patient information

4.5.3 maintain the security of confidential and/or sensitive information, including that stored on communication devices

4.5.4 not disclose, use or take advantage of information obtained in the course of official duties, including when they cease to work in NSW Health.

5 Key concepts

Privacy law uses a range of general terms and concepts. In many instances these concepts will help you decide if the legislation applies to the activity you are pursuing, or determine how you should act in dealing with personal health information. Some of the most important concepts are set out below.

5.1 Health information

Health information is personal information or an opinion about:

- a person's physical or mental health or disability, or
- a person's express wishes about the future provision of health services for themselves, or
- a health service provided, or to be provided, to a person.

Any personal information collected for the purposes of the provision of health care will generally be "health information". It will also include personal information that is not itself health-related but is collected in connection with providing health services or connected in association with decisions to donate organs or body substances.

The *HRIP Act* also specifically includes genetic information about an individual that predicts or could predict the health of the individual or of their genetic relatives. A genetic relative means a person who is related to an individual by blood, for example, a sibling, parent or descendant of the individual. See Section 11.2.3.4 Genetic information.

Under the *Health Records and Information Privacy Regulation 2012*, a health service includes:

- services provided by an accredited chaplain or pastoral health worker, including volunteers, in a public hospital or a health institution controlled by a public health organisation, and
- research services conducted by or on behalf of the Ministry, the Health Administration Corporation, a public health organisation or public hospital, the Cancer Institute (NSW) or by another organisation pursuant to an agreement with the Ministry, the Health Administration Corporation, a public health organisation or public hospital or the Cancer Institute (NSW).

The *HRIP Act* uses the term 'health information' to mean health information that identifies or could potentially identify an individual. This Manual has, however, adopted the term "personal health information", to emphasise that neither the *HRIP Act* nor the Manual regulates the collection, use or disclosure of other health-related but non-identifying information, such as de-identified and statistical data. The requirements of the Manual do not need to be followed in relation to this type of information.

5.2 Personal information

Personal information is defined in Section 4 of the *PPIP Act* as:

> *"any information or an opinion about a person whose identity is apparent or can reasonably be ascertained from the information or opinion"*

If a person's identity cannot be ascertained from the information it will NOT be personal information, and the privacy laws will not apply.

Unique identifying information such as name and address, photographs, biometric information including fingerprints and genetic characteristics are "personal information". A range of other information can also become personal information, if it is viewed in combination with other information, which together is sufficient to allow a person's identity to be "reasonably ascertained". Characteristics which may fall into this category include age, date of birth, ethnicity and diagnosis. The potential for these types of general information to become identifying is higher when dealing with a small population, or dealing with unusual or rare clinical conditions.

Example: States and Territories are asked to provide information for a national data collection, covering certain conditions in a specific area of medicine. The collection does not intend to collect "personal information", but only the numbers per state and clinical information. Given the information is neither identifying nor potentially identifying, privacy laws do not need to be considered when determining whether to participate in the collection.

Another similar data collection is proposed, this time seeking more details of certain rare genetic conditions. In this case, the rare occurrence of these conditions and the additional information requested may be sufficient to identify specific individuals with these types of conditions. As a result, privacy law, and the grounds allowing disclosure in HPP 11, would need to be considered in deciding whether to participate and provide data.

The definition of personal information is much broader than that of personal health information, and is regulated by the *PPIP Act*. The legislative requirements for managing general personal information are different from the requirements for managing personal health information, and are not covered by this Manual. Guidance for NSW Health staff on the management of personal information is contained in the NSW Health Privacy Management Plan.

Further guidance:
- PD2005_554: NSW Health Privacy Management Plan

The obligations under privacy legislation apply to anyone who "holds" information. A health service holds personal health information if the information is in its possession or control. This includes situations where the information is not stored on the organisation's premises, but is available and access to the information is controlled by the health service.

Privacy laws also extend the coverage of privacy rules to information related to a deceased person for up to 30 years after their death.

Privacy legislation specifically excludes certain information from the definition of 'personal information'. For example:

- information that is generally available to the public, for example in a publication, library, or the NSW State Archives
- information that is protected under other laws, such as a Protected Disclosure, information about a witness on a protected witness program or information obtained under certain special police operations.

5.3 De-identified information

De-identified information is information or opinion about a person whose identity is not apparent and cannot be reasonably ascertained from the information or opinion.

If there is a reasonable chance that the information is potentially identifiable, it cannot be classified as de-identified. Clearly, whether information can be considered de-identified will be dependent on the specific circumstances which arise in any disclosure.

Example: Data on small or unique groups, particularly in rural areas, may not be de-identified even where identifiers have been stripped.

De-identified information is exempt from privacy law and from the requirements of this Manual. The Health Privacy Principles do not apply to de-identified information.

5.4 Consent

Consent is an important element in health care provision and in dealing with health privacy issues. Obtaining consent represents good clinical practice as it involves patients directly in their health care decisions and provides a mechanism for exchange of information about both the patient's wishes and personal perspective and the clinical or other issues which may indicate to their service provider that information should be shared.

5.4.1 Elements of consent

- A consent should be **informed**. That is, there must be reasonable efforts to ensure that the person concerned has the information they need to understand what they are consenting to, why it is necessary or desirable, and what may be the results both of giving and withholding consent.
- In order to be informed, the consent should also be **reasonably specific**. Reliance on general or blanket consents can be problematic if the patient later indicates they were not informed of the particular usage proposed.
- A consent should be **freely given**. That is, the person must not be coerced, pressured or intimidated. They should not feel they have no choice or that they do not have enough time to make up their mind.
- A consent should only be sought from a person who has **capacity** to consent (see Section 5.5 Test for capacity).
- A consent should be **timely.** The validity of the consent is dependent on the patient's expectation. For example, if it is a standard consent for all patients, the validity may be 12 months or longer if the patient is accessing ongoing services. However, if the consent is for a specific use and disclosure of information, the recommended timeframe is 3 months.

The validity of a consent is more likely to be questioned where a lengthy period of time has passed or the patient's personal situation has changed so markedly that there are grounds to suggest their views may have changed. Reasonable steps must be taken to ensure that the reason for disclosure directly relates to the terms of the consent.

- Consent can be obtained **in writing or verbally in person**, but when obtained verbally should always be recorded, for example, by a notation in the patient's health record.

5.4.2 Implied consent

Implied consent generally means that a person has not explicitly, either verbally or in writing given their agreement, but through their conduct or behaviour have "implied" consent, or by consenting to one action, they have impliedly consented to a range of other activities. The application of implied consent is limited. It will generally only arise in situations where a person's consent to treatment can be implied to include consent to other uses and disclosures of information necessary to provide the care.

Example: A patient provides a detailed consent to medical treatment. This consent includes consent for a range of pathology tests required to be performed as part of the episode of care. In doing so, the patient is also giving an implied consent for any information necessary to have the test performed to be provided to the pathology service provider, and if pathology results require action, the pathology service will convey the positive result to the appropriate service provider or identified specialist service responsible for follow up with the patient as part of the continuum of care.

Further guidance

- PD2005_406: Consent to Medical Treatment – Patient Information

5.4.3 Express consent

Express consent generally requires documentation of a consent which shows specific and clear intention on the part of the patient. A formal written consent will meet this requirement, provided the activity being consented to is accurate, precise and clearly expressed. There are two circumstances where the HRIP Act requires "express consent" from the patient. These are:

- under HPP 4, where a person can waive their right to be given information regarding the collection of their personal health information (see Section 7.4.1.2 The person waives their right to be told) and
- under HPP 15, where a person consents to participate in a state or national EHR system (see Section 13.3 Linkage of health records (HPP 15)).

5.4.4 Deciding if consent is needed

Privacy law recognises there are a range of circumstances when consent is not required to lawfully use or disclose information. The most important examples include where:

- the health service is using or disclosing the information for the **primary purpose** for which it was collected (see Section 11.1 Use and disclosure for the "primary purpose")
- the health service is using or disclosing the information for a **directly related secondary purpose**, and the patient would **reasonably expect** that use or disclosure. Reliance on a "directly related purpose" depends on what the patient would expect to happen to his or her information. As such it is important to ensure information about how the health service uses and discloses information is readily available for patients (see Sections 7.4 Informing individuals about what is collected (HPP 4) and 11.2 Use and disclosure for a "secondary purpose")
- the health service is **lawfully authorised** or required to use or disclose the personal health information (See Section 11.3 Use and disclosure authorised by law (HPPs 10(2) and 11(2))).

Some examples of when patient consent is not required include where:

- access to the information is being requested under a court subpoena or search warrant
- release of a discharge summary to a patient's GP where the patient (or their authorised representative) has provided the GP's details
- for current and future ongoing care and treatment purposes where the patient has been made generally aware that their information may be used in this way
- use and disclosure of a patient's genetic information is permitted to their genetic relatives in certain circumstances prescribed in guidelines issued by the NSW Privacy Commissioner, Information and Privacy Commission NSW (see Section 11.2.3.4 Genetic information)
- in emergency situations.

These and other situations where use or disclosure does not require consent are addressed in more detail in Section 11.

5.5 Test for capacity

5.5.1 General rule

A person cannot give consent, or make other decisions under privacy law if they do not have the necessary capacity to do so. Incapacity can be due to age, injury or illness, or physical or mental impairment. While it is a permanent condition for some people, it may be a temporary condition for others.

The *HRIP Act* establishes a test for capacity which states a person is incapable of giving consent if they:

- cannot understand the general nature and effect of the matter they are being asked to decide on or
- cannot communicate their intentions about that matter.

The test does not therefore impose arbitrary rules dictating capacity on the basis of mental illness, disability or age. It requires a professional assessment of the individual's ability to make a specific decision. The complexity, seriousness and long-term impact of any decision will impact on the level of understanding required in any particular case.

5.5.2 Minors

A minor is a person **under the age of 18 years old**. When considering issues of access to, or disclosure of, health records relating to minors, the treating health practitioner should assess the maturity of the patient, in particular their ability to understand the content of the records and consequences of their decision. The following principles can be used as an age guide:

- Where a patient is less than 14 years of age, consent (for access to, or disclosure of, the child's health record) given by a parent or legal guardian is generally necessary. In some circumstances, consent can be made by the young person if he or she is considered by the treating health practitioner mature enough, and if this would be appropriate in the circumstances.
- Where the patient is between 14 and 16 years of age, the young person is generally able to consent to access to, or disclosure of, their own health record. Effort should be made to seek the consent of a parent or legal guardian unless the patient indicates a strong objection, and this is reasonable in the circumstances.
- Where the patient is 16 years of age or over, they should generally be capable of consenting to access to, or disclosure of, their own health record for themselves.

Before disclosing the records of a minor, health staff should consider the content of the record and whether the minor may have any objections to its release. Consideration should be given to consulting with the minor prior to disclosure.

When deciding if a person has capacity, you must consider whether they would be able to give consent if given appropriate assistance. The rationale for the decision as to whether a person has capacity or not should be recorded in their health record.

If a person, including a minor, does not have the capacity to decide for themselves, an "authorised representative" can give consent on their behalf.

Further guidance

- Section 5.6.1.1 Where the health service is aware that parents are divorced or separated

5.6 Authorised representative

The concept of 'authorised representative' is an integral component of health privacy law. An authorised representative is able to make decisions relating to access to, or disclosure of, health records on the patient's behalf where the patient lacks capacity to make these decisions for themselves (see Section 5.5 Test for capacity).

In order to ascertain who may act as a patient's authorised representative, health services should not rely on the person indicated in the health record as 'person to contact' or 'next of kin'. It is generally necessary to review a patient's health record to determine who may be appointed as their authorised representative, in accordance with the hierarchy set out in the *HRIP Act* below (see Section 5.6.1 Hierarchy for appointing 'authorised representative').

Appropriate personal identification and any relevant documentation (for example, current enduring power of attorney, enduring guardianship documents, or if deceased, a certified copy of the patient's will displaying the executor details) should be provided prior to the disclosure of, or access to, personal health information relating to a patient.

Staff should liaise with the Health Information Service for their health service for assistance with this process.

5.6.1 Hierarchy for appointing 'authorised representative'

The *HRIP Act* sets out the list of people who can be an authorised representative on behalf of a patient who lacks capacity. They are:

- someone who has an '*enduring* power of attorney' for the individual or
- a guardian, including someone with 'enduring guardianship', as defined in the *Guardianship Act 1987* or
- if the individual is a child under 18, a person who has parental responsibility for them. The Act defines this as "all the duties, powers, responsibility and authority which, by law, parents have in relation to their children" or
- a "person responsible" under Section 33A of the *Guardianship Act 1987* or
- any other person who is authorised by law to act for or represent the person

Generally, the role of an authorised representative lapses when the patient dies, unless the law expressly provides for it to continue. Powers of attorney, for example, have no effect after the person who made them has died. The most common situation where an authorised representative may have authority to act after death is in the case of an executor or administrator of a deceased estate. Their legal authority arises after death, and continues until such times as the estate is settled or distributed.

Who is a "person responsible" is determined via a hierarchy set out by the *Guardianship Act 1987*, as follows:

- If the person is under guardianship, the guardian is the person responsible
- If there is no guardian, an enduring guardian appointed by the patient with authority to make decisions regarding medical care
- If there is no enduring guardian, a spouse (including a de facto spouse) with whom the person has a close continuing relationship is the person responsible
- If there is no guardian or spouse, a person who has the care of the patient unable to consent is the person responsible. Such a person is regarded to have the care of the patient if they have provided, or have arranged to be provided, domestic services and support otherwise than for remuneration. Where the patient has been cared for by a person in a nursing home, hostel, boarding house or other group accommodation, that person does not have care of the person. In such cases the patient remains in the care of the person he or she was immediately with before residing in the institution
- If there is no guardian, spouse, or carer, a close relative, including adult children, or friend may act as the person responsible provided they are not receiving remuneration for any services provided.
- If the person is in the care of the Secretary under s13 of the *Guardianship Act 1987*, the Secretary is the person responsible.

Further guidance

- Section 1 Definitions & acronyms
- Section 11.2.2.1 Where a third party seeks access
- Section 11.2.9 Disclosure on compassionate grounds
- Section 12 Patient access and amendment (HPPs 6, 7 & 8)

5.6.1.1 Where the health service is aware that the parents are divorced or separated

Where the health service is aware that parents are divorced or separated, "parental responsibility" may be altered. Consideration needs to be given to the terms of any parenting order issued by the Family Court, and a copy of the order should be retained on the child's health record. Parenting orders have replaced custody and access orders, and will set out the responsibilities and role of each parent.

Where there is no parenting order, both parents will retain parental responsibility for the children. This means that both parents are independently permitted to consent on the child's behalf.

Further guidance

- Section 12.3.1.3 The disclosure of personal information about a child would not be in the best interests of the child
- Section 12.5.1 Parenting orders

5.6.1.2 Next of kin

'Next of kin' is a term sometimes used across the health system to allow a patient to nominate their partner or a relative as a person to contact. Typically, the name, contact details, date of birth and relationship to the patient of the 'next of kin' are collected and recorded by health facilities.

The *HRIP Act* does not use or rely on the term 'next of kin'. It does not therefore give a "next of kin" any authority to make decisions on behalf of the patient. Where a person is listed as a "next of kin", the health practitioner should check whether they are an authorised representative (see above) before relying on that person to make a decision on behalf of the patient.

5.7 "Reasonable and practicable"

The *HRIP Act* often qualifies requirements by reference to what is reasonable or practicable. These are concepts that cannot be readily defined as they will vary depending on the circumstances arising. There are however certain matters which can be considered in any case in deciding if something is "reasonable" or "practicable".

- Consider what **most lay people** (not a health professional) may expect, or think acceptable, in this situation
- Take into account the **context**, and all the surrounding circumstances. Will the activity have a major impact on the patient or others? Is a person's physical safety at risk? Is the issue urgent?
- In assuming that an action is **reasonably necessary**, consider whether there are other ways of achieving the desired result
- Assess the **cost and time** involved in complying, and whether they are appropriate having regard to the benefits or risks
- Do not assume that something is not reasonable or practicable simply because it is **inconvenient or a nuisance** (this is not an acceptable justification).

5.8 'Sensitive' information and patient expectations

All personal health information is generally considered to be sensitive personal information, dealing as it does with matters that are extremely personal and which a patient will generally expect to be shielded from public disclosure. The terms of the *HRIP Act* are based on adopting and reflecting these expectations. The *HRIP Act* does not classify certain types of personal health information as being more sensitive than other types, except where other statutory obligations apply to require that certain information receives a greater level of protection, for example,

- HIV/AIDS-related information, see Section 4.1.3.2
- Adoption information, see Section 15.9.2

The *HRIP Act* requires that personal health information is treated in accordance with an individual's reasonable expectation, and that reasonable steps are taken to inform a patient of how he or she can expect their information to be handled.

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. Health staff should not make assumptions about what a patient might consider 'sensitive'.

Health staff should make special efforts as are reasonable in the circumstances to explain to patients how patient information is generally used and disclosed.

Health services should manage an individual's personal health information in accordance with privacy rules.

Further guidance

- Section 7.4 Informing individuals about what is collected (HPP 4)
- Section 11.2.1.2 'Reasonable expectation'

5.8.1 Specific health services

In the case of some specific health services, such as genetics services, drug and alcohol services, or sexual health services for example, it may be appropriate to manage personal health information differently to general health services, given the more sensitive nature of the information and the patients' expectation as to how their personal health information may be handled in these circumstances.

Further guidance

- Section 15.9 Information-specific laws and policies

5.8.2 Patient requests

In rare circumstances, a patient may make a special request that their personal health information is not used or disclosed for purposes as allowed by the *HRIP Act* and described in this Manual. When health service staff receive such a request, it will be situation specific and the professional judgment of local health service staff will be required to resolve such requests, for example, it may be necessary to balance the implications of meeting the request with the capacity to provide safe and appropriate health services.

Further guidance

- Section 11.2.1.3 Outside a patient's 'reasonable expectation'

5.8.3 'Sensitive' information – non-personal

NSW Health agencies may hold sensitive information which is not personal health information, such as tender documents, private hospital licensing information or documents detailing government relations. These documents require secure document management in accordance with the *State Records Act* including the General Retention and Disposal Authority (GDA 21). This authority applies to records created and maintained to support the management and delivery of public health care services and programs.

Where, as in most cases, these documents do not contain personal health information, the terms of the *HRIP Act* and this Manual will not apply.

6 Responsibilities under privacy law

Policies and procedures are of little value if not routinely observed in practice at the service level. Ultimately, if a high level of information privacy is to be maintained, a personal commitment is required from health staff.

It is essential that health staff be made aware of their individual rights and responsibilities in respect of safeguarding information privacy. They need to be informed about patients' rights of privacy and access to their own information. The importance of basic observances cannot be over-emphasised, such as not discussing patients publicly in a manner that would allow identification of individuals or small groups, keeping passwords secure, and taking such measures as to protect the security of patient information in electronic health record systems from unauthorised access.

6.1 Chief Executives

6.1.1 Key obligations

- to ensure that all staff members are aware of the requirements of this Manual
- to ensure all staff members undertake appropriate privacy training
- to ensure that all staff members have access to appropriate material about their privacy obligations, including the Privacy Information Leaflet for Staff (see Appendix 6), NSW Health Privacy Manual for Health Information
- to meet statutory annual reporting requirements regarding privacy compliance and applications for internal review (see Section 6.7 Privacy annual reporting)
- to designate a specific officer for the health service to whom requests for guidance on information privacy should be referred and who should support staff in ensuring privacy policies and procedures are observed.

6.1.2 Staff training

Staff awareness of privacy issues should be promoted in a routine and ongoing way. Methods of doing this will vary, depending on the type of information and other characteristics of the local environment.

All staff should be provided with the *NSW Health Privacy Information Leaflet for Staff,* see Appendix 6.

Staff should undertake privacy training in order to understand their obligations in relation to privacy principles and requirements. It is the responsibility of health services to provide and promote such training. Face-to-face training can be arranged by contacting the local Privacy Contact Officer or Learning and Development Unit.

Two privacy online training modules are also available via the NSW Health Education and Training Institute (HETI) website: www.heti.nsw.gov.au/courses/

6.1.3 Mandatory training

All NSW Health staff are required to complete one of the two privacy online training modules as part of their mandatory training requirements. The mandatory training module is entitled 'Privacy module 1 – Know your boundaries' available at: www.heti.nsw.gov.au/programs/mandatory-training

The expected duration to undertake this training module is approximately 20 minutes.

Staff should undertake this training as part of orientation within 1 month of commencement as a NSW public health system employee.

There is no requirement to repeat the privacy mandatory training module, unless otherwise required as part of a remedial process, or as a result of updates made to the mandatory training module following any changes to policy.

Further guidance

- PD2014_023: Mandatory Training Requirements in Policy Directives

6.1.4 Staff communication and alerts

Staff must also be informed and regularly reminded of their responsibilities to patient privacy and confidentiality. This can be achieved through a combination of staff induction, staff meetings, training, staff newsletters, notices, posters, and so on.

Building alerts and notifications into electronic systems may also assist to inform staff of their privacy obligations. Providing staff with brief privacy messages at critical decision points in the system may be an effective way of reminding staff of privacy obligations.

Some examples of electronic notifications for NSW Health staff are:

"Remember you must only access the information necessary to fulfil your work duties. If in doubt, check with your senior manager, or for further information go to: www.health.nsw.gov.au/patients/privacy"

"You are bound by strict privacy law and NSW Health privacy policies regarding access to, use and disclosure of the personal health information contained in <ABC> system.
*The principal governance policy governing <ABC> system is: <XYZ>
*The principal privacy policy is: NSW Health Privacy Manual for Health Information.
*The principal privacy law is: *NSW Health Records and Information Privacy Act 2002*"

"If you suspect a breach of the privacy or security of the <ABC> system, you should discuss this with your manager, and consider contacting the Privacy Contact Officer for your organisation. Details are available at: www.health.nsw.gov.au/patients/privacy"

6.2 Privacy Contact Officer

Each health service should have a Privacy Contact Officer (PCO) to facilitate compliance with privacy law and NSW Health privacy policy in their health service.

The principal tasks for Privacy Contact Officers are:

- act as a first point of contact for members of the public for matters related to privacy
- serve as a focal point for health service staff for matters related to privacy
- act as a first point of contact with the NSW Ministry of Health and Privacy NSW for matters related to privacy
- ensuring privacy complaints and requests for internal review are dealt with in accordance with the NSW Health Internal Review Guidelines (GL2006_007)
- disseminating information on privacy matters within the health service
- arranging privacy education and training for health service staff.

Further guidance

- Listing for NSW Health Privacy Contact Officers is available at: www.health.nsw.gov.au/resources/utilities/privacy/contacts_pdf.asp

6.3 Other staff

6.3.1 Managers and supervisors

- should provide leadership and direction to ensure the Manual is effectively implemented in the units or by the staff they are responsible for
- should monitor the quality and effectiveness of management and use of personal health information and take appropriate action to address any risks, gaps or shortcomings
- should ensure staff responsible for management and use of personal health information have the skills and support they need to effectively comply with privacy law, including access to privacy education
- should include privacy provisions in policies, procedures and service or project plans wherever appropriate
- should refer privacy complaints and requests for privacy internal review to the Privacy Contact Officer for the health service
- should be aware of local protocols as to when to refer requests for access to and disclosure of personal health information to the local Health Information Service.

6.3.2 Health care providers

- should implement and comply with the *HRIP Act* and this Manual
- should take responsibility for complying with the *HRIP Act* and this Manual and for keeping up to date with any changes
- should report potential or actual breaches, risks, or other issues that may occur in relation to personal health information.

6.3.3 Funding and grants administrators

- should ensure funding processes, conditions and reporting requirements comply with privacy law
- should monitor the protection of personal health information in programs and initiatives funded by the public health system and initiate appropriate action to address any risks or shortcomings.

6.3.4 Information systems and information technology managers

- should ensure that the development and modification of information technology systems comply with privacy law
- Should ensure that all documentation and processes for IT policy, procedures and governance are consistent with privacy law.

6.4 Contracted agencies

A responsible representative of a contracted agency, where the service necessitates accessing personal health information, should sign an undertaking to comply with the *HRIP Act* or equivalent law as part of the conditions of their contract (see Appendix 3 Pro forma Privacy undertaking). The agreement should clearly set out responsibility for data security in transit and requirements for secure storage. Individuals working for the agency should also sign undertakings where their tasks will involve direct access to personal health information.

Examples of key privacy criteria appropriate for inclusion in any such contract are as follows:

- an undertaking not to knowingly access any personal health information unless such information is essential to properly and efficiently perform contractual obligations
- an understanding that access to, holding and use of personal health information is subject to the Health Privacy Principles contained in the *Health Records and Information Privacy Act 2002*

- an undertaking to comply with the Health Privacy Principles and relevant NSW Health policies affecting the collection, holding, use or disclosure of personal health information
- an undertaking not to divulge any personal health information regarding individual persons, except as allowed by the Health Privacy Principles
- an undertaking to follow other information privacy and security procedures as stipulated by NSW Health policies in relation to any personal health information accessed in the course of contractual obligations
- an undertaking to ensure that, so far as is possible, such information, whether in the form of paper documents, computerised data or in any other form, cannot be viewed by unauthorised persons, and that the information is stored in a secure and orderly manner which prevents unauthorised access
- an undertaking to inform a supervisor/NSW Health contact immediately in the event of any breach of privacy or security relating to personal health information accessed in the course of contractual obligations.

The above criteria are set out in pro forma privacy undertakings, provided in Appendix 3.

Where possible original source data should not be sent off premises. Where this is necessary, detailed records of source documents should be kept and thorough checks made when returned to ensure that all records are returned.

6.5 Compliance tips

There are a number of ways health services can support their staff to meet the obligations under the Act. Some **options** include:

- Include privacy education and training as part of staff orientation
- Include an overview of staff privacy obligations and list of key privacy resources in staff handbook or 'Survival Manual' for new staff (see Section 6.6 NSW Health privacy webpage and key privacy resources)
- Ensure all new staff receive and are given an opportunity to read and respond to the Privacy Information Leaflet for Staff (see Appendix 6)
- Provide information sheets/ posters for staff providing contact details for privacy enquiries. Ensure that all staff know to liaise with their Privacy Contact Officer regarding privacy complaints, including requests for internal review (see Section 14 Complaints handling)
- Develop standard privacy undertakings for staff and student access to health records, in particular electronic health record systems (see Appendix 3)
- Establish a Privacy Advisory/ Working Group to oversee privacy management within the health service (to include Privacy Contact Officer, Training Coordinator, Health Information Manager, other interested staff)
- Maintain an up-to-date privacy information webpage for your health service. The NSW Health Privacy web page can be used as an example (see Section 6.6 NSW Health privacy webpage and key privacy resources).

6.6 NSW Health privacy webpage and key privacy resources

The NSW Health Privacy webpage contains resources to assist health services with interpreting and complying with privacy law.

Key privacy resources available are:

- NSW Health Privacy Manual for Health Information
- NSW Health Internal Review Guidelines, GL2006_007
- Privacy Leaflet for Patients
- Privacy Information Leaflet for Staff

- Privacy Online Training Program
- Privacy Newsletter
- NSW Health Privacy Management Plan
- Link to *Privacy and Personal Information Protection Act 1998*
- Link to *Health Records and Information Privacy Act 2002*
- Link to NSW Privacy Commissioner's Statutory guidelines pursuant to the *HRIP Act*, Information and Privacy Commission NSW

The NSW Health Privacy webpage can be found at:
www.health.nsw.gov.au/patients/privacy/Pages/default.aspx

6.7 Privacy annual reporting

It is a statutory requirement that public agencies, including local health districts (LHDs) and public health organisations (PHOs) comprising NSW Health, publish details of privacy matters as part of their annual reporting obligations.

Statutory requirements for annual reporting on privacy matters are set out in clause 6 of the *Annual Reports (Departments) Regulation 2010, and in clause 10 of the Annual Reports (Statutory Bodies) Regulation 2010*.

The privacy annual report of each agency must include:

- a statement of the action taken by the agency in complying with the requirements of the *Privacy and Personal Information Protection Act 1998*, and the *Health Records and Information Privacy Act 2002*, such as the delivery of privacy education and training to staff, the distribution of information regarding privacy to patients, and so on.
- statistical details of any Internal Review(s) conducted by, or on behalf of, the agency, including:
  - when the application for each Review was received
  - whether it was found that any privacy principles were breached and
  - whether the applicant sought further review in the NSW Civil & Administrative Tribunal.

Care must be taken to ensure that the details included in the annual report can in no way identify an applicant of Internal Review.

The report should be completed annually by 31 October, and be published with Chief Executive (or delegate) approval via the agency's privacy website. A copy should also be provided to the NSW Ministry of Health Legal and Regulatory Services Branch.

7 Collecting personal health information (HPPs 1–4)

Everyone who has direct contact with patients may have some role in collecting personal health information. Those not involved in direct service provision, such as admissions clerks, may also collect information.

7.1 When can you collect information? (HPP 1)

While privacy laws impose some controls over when personal health information can be collected, these will not affect the core business of NSW Health.

The laws clearly allow health services and health staff to collect personal health information for purposes relating to health care and treatment.

Health services are established under the *Health Services Act 1997.* Some of the key functions set out in that *Act* include:

- to provide relief to sick and injured persons through the provision of care and treatment
- to promote, protect and maintain the health of the community
- to conduct and manage public hospitals, health institutions, health services and health support services under its control
- to achieve and maintain adequate standards of patient care and services
- to ensure the efficient and economic operation of its health services and health support services and use of its resources
- to investigate and assess health needs in its area
- to plan future development of health services in its area
- to provide education and training relevant to the provision of health services
- to undertake research and development relevant to the provision of health services.

When collecting personal health information you should consider these functions. Information can only be collected if the purpose of collection is directly related to what the agency does and the collection is necessary for those purposes.

Example: Collecting details of a patient's income is unlikely to be necessary for provision of public health services. Collection of information about pensioner or veteran status may however be necessary, if this information impacts on patient entitlements.

Information cannot be collected by an "unlawful means".

Example: Information cannot be collected through recording a conversation without a person's consent, as this would breach laws relating to listening devices in NSW.

7.2 How should information be collected? (HPP 2)

HPP 2 requires a health service to take reasonable steps to ensure:

- the information collected is **relevant to the purpose, is not excessive and is accurate, up to date and complete**, and
- collection of the information does not **unreasonably intrude** on the personal affairs of the individual.

This means that health services should be sensitive to, and take all reasonable steps to minimise, intrusion on the people from whom they collect personal health information. Particular care should be taken when it is clear the information may be personal, distressing or embarrassing to the patient concerned.

Example: Information about a mental illness is requested from a patient while sitting in the open reception area of a community health service. Other patients waiting to be seen can hear the discussion clearly, and the patient is uncomfortable. You should seek to collect the information in an environment where the potential for other people to overhear details is minimised, for example, using another room if available, or taking him aside to discuss privately.

Example: Doctors in a crowded emergency department request information from a patient who has just been brought in with a serious injury. Given the urgency of the situation, it may be appropriate for the medical staff to obtain this information, regardless of the fact that other people may overhear.

7.3 Who should information be collected from? (HPP 3)

Personal health information must be **collected from the person** it relates to, **unless it is unreasonable or impracticable** to do so.

Example: A frail but alert elderly woman is accompanied to admissions by her son. Her son requests that you address questions to him, out of his mother's hearing, as he feels this will be quicker and less distressing for her. You should not proceed in this way purely on the basis of the son's request. If the woman is able and willing to provide this information, you should obtain it from her.

If the elderly woman indicates that she wants her son to answer for her, you should try to make sure she understands and is involved.

Common examples of where it may be **unreasonable or impracticable** to collect personal health information directly from the person it concerns include:

Taking an individual or family medical history for your patient, where you require information about sibling illness or medical history to assist in making a diagnosis and providing care to your patient.

Where patient lacks capacity and that lack of capacity impairs their ability to give you necessary information, you may collect it from an authorised representative.

Where the person is seriously injured or in a coma due to an accident and cannot communicate, the necessary information can be collected from a family member, paramedic or other person who may have seen the accident.

Where the information is obtained from another health practitioner as part of a referral.

7.4 Informing individuals about what is collected (HPP 4)

7.4.1 Who do you need to inform if you have collected the information?

Generally, you should tell the person to whom the information relates what is collected, by whom, how it will be used, and their rights in relation to it.

This applies irrespective of whether the information was collected from a third party, or directly from the person concerned.

The law recognises there will be situations when it is not reasonable or appropriate to do this.

Those examples of most relevance to health services are set out below.

7.4.1.1 The person to whom the information relates lacks capacity

If the person to whom the information relates is not capable of understanding the information provided to him or her regarding the collection, security, use and disclosure of his or her personal health information, this information can be given to the person's authorised representative.

Where you need to deal with an authorised representative it is still good practice to explain the points to the person to whom the information relates in a way that is appropriate to their level of understanding. This is to enable the person to be involved in the notification process to the greatest extent possible.

7.4.1.2 The person waives their right to be told

If the person expressly waives their right to be told information regarding the collection, security, use and disclosure of his or her personal health information, HPP 4 does not need to be complied with. HPP 4 requires this consent to be an "express consent", so any such waiver should be recorded to enable later verification.

7.4.1.3 Informing a person will prejudice their interests or pose a threat

You do not need to tell someone you have collected information about them if this would pose a serious threat to life or health, prejudice the individual's interests, prejudice law enforcement or investigative activities.

Example : If you had collected information about the drug dependency of a violent spouse as part of providing advice and support to a domestic violence victim, you would not be required to tell the violent spouse you had collected the information, if it would place your patient, yourself or another person at risk

7.4.1.4 Where the information is collected from a third party

Health services do not have to inform an individual about information they have collected about them from a third party if:

- the information was collected from a third party because it was unreasonable or impractical to collect it from the individual, and it would also be unreasonable or impractical to inform the individual about the collection
- the information was collected in the process of recording a family, social or medical history, and this was necessary to provide health services to the patient
- the information is collected from an authorised representative because the health service believes that the individual is incapable of understanding the nature of the information required
- the information was initially collected by another agency or organisation and there are reasonable grounds to believe that the individual has already been informed of the necessary information by that other agency or organisation.

When information should be provided in these circumstances is governed by Statutory guidelines issued by the NSW Privacy Commissioner, Information and Privacy Commission NSW.

Further guidance

- NSW Privacy Commissioner's *Statutory guidelines on notifying a person when you have collected health information about them from someone else*, available at: www.ipc.nsw.gov.au/privacy/ipc_legislation

7.4.2 What information do individuals need to be told?

Except for the circumstances outlined above, Health Privacy Principle (HPP) 4 requires that individuals must be told certain information at the time, or as soon as practicable after, their personal health information is collected. The information that individuals must be told is:

- the **identity of the health service** collecting the information and how to contact it
- the **purposes** for which the information is collected
- **who the health service usually discloses information** of that kind to
- **other laws** that require the particular information to be collected
- an individual's right to **request access** to information held about them
- consequences, if any**, if all or part of the information is not provided**.

Further guidance

- Section 7.4.5 – Privacy Leaflet for Patients – Development
- Appendix 5 – Pro Forma Privacy Leaflet for Patients

7.4.3 When should individuals be told?

The information should, where practicable, be given to patients before, or at the same time, as the information is collected.

If it is not practicable to inform the individual at the time the information is collected the health service should do what it reasonably can to inform the individual subsequently.

7.4.4 How should individuals be told?

It is the responsibility of the agency which collects personal health information directly from the patient (or their representative), normally a health service, to inform individuals about how they can expect their personal health information to be treated.

Information can be provided in a variety of ways, including:

- 'Privacy Leaflet for Patients' (see Section 7.4.5) to be made available to all patients
- Verbal reinforcement or explanation of 'Privacy Leaflet for Patients' where necessary
- Privacy poster (see Section 7.4.6) and counter notices displayed in public areas of health services
- Information included on admission forms
- Information provided on the health service's website.

This information should be prominently displayed, readily and easily accessible to patients, in admission areas, community health reception areas, hospital wards, outpatient waiting rooms, Emergency Department waiting rooms and in all public access areas where patients receive services.

Health services should not rely only on verbal communication of this information unless the circumstances provide no alternative. If information is only provided verbally, a written note should be made in the health record to ensure a contemporaneous record is kept of the information provided.

7.4.5 Privacy Leaflet for Patients – Development

The NSW Health 'Privacy Leaflet for Patients' sets out the general information which should be provided to patients. This information must be presented in a format and in language that they can understand. The leaflet should be adapted by health services to include local health service contact details.

The proforma leaflet may be further adapted to accommodate specific services which may have additional or different information sharing needs and patient expectations to address. Examples of such services include, but are not limited to, palliative care, mental health, drug and alcohol, sexual health, genetics services, and services for young people (see Section 7.4.7 Youth-friendly privacy resources). If the service is linked to a particular Commonwealth program, or if routine reporting is required, this should also be included.

In all cases, the leaflet must cover the criteria listed in Health Privacy Principle 4 (see Section 7.4.2 What information do individuals need to be told?). It should also be sufficiently clear to allow the patient to readily assess and understand the circumstances when their information may be shared, for example, whether it is shared with a wider treating team.

Circumstances for sharing patient information to be listed in the leaflet must not extend beyond the primary, secondary and lawfully authorised purposes described in Section 11.

When adapting the pro forma privacy leaflet, health services should contact their local Privacy Contact Officer, to ensure the adaptations remain within the parameters of the Health Privacy Principles.

For copies of the local privacy leaflet or any other related enquiries, staff should liaise with their Privacy Contact Officer in the first instance.

A contact list for NSW Health Privacy Contact Officers is available via the NSW Health privacy webpage at: www.health.nsw.gov.au/patients/privacy/Pages

The pro forma leaflet is also available via this webpage and an example is also provided in Appendix 5 of this Manual.

The pro forma 'Privacy Leaflet for Patients' is available in 29 community languages via the NSW Health Privacy website, or via the Multicultural Health Communication Service website at: www.mhcs.health.nsw.gov.au/

7.4.5.1 Privacy Leaflet for Patients – Distribution

The privacy leaflet should be readily available to all patients receiving NSW Health services.

In addition, copies of the privacy leaflet should be clearly displayed and available in all hospital and community health service public waiting areas. Copies of the leaflet may also be provided at the bedside, and included in any 'Information Pack' sent to patients scheduled for admission to hospital.

Depending on the nature of the health service being provided, patients accessing a health service for the first time should be provided with the leaflet at the time of their initial consultation, accompanied with some verbal explanation as to how the individual's personal health information may be used and disclosed.

Further guidance

- Section 7.4.2 – What information do individuals need to be told?
- Section 11 – Using & disclosing personal health information (HPPs 10 & 11)
- Appendix 5 – Pro forma Privacy Leaflet for Patients

7.4.6 Privacy poster

The NSW Health Privacy Poster should be displayed in public areas, such as in Emergency Department waiting rooms, Outpatient and Community Health waiting rooms. In addition, the Privacy Poster should be displayed, where appropriate, in wards, corridors, at information points, concierge, nurse stations, and so on.

Please contact the Privacy Contact Officer for your health service for copies of the Privacy Poster.

7.4.7 Youth-friendly privacy resources

Research documented in the NSW Youth Health Policy has shown that one barrier to prevent young people accessing health services is uncertainty regarding confidentiality of health information.

Youth-friendly confidentiality resources, including a poster, pocket-sized-card, and online fact sheet, have been developed by NSW Kids and Families to inform young people (aged 12-24 years old) about the confidentiality of their health information.

Health staff are encouraged to provide all young patients with the youth-friendly privacy brochure, and to discuss any privacy concerns or questions.

The Youth-friendly confidentiality resources are available via:

- NSW Health 'Better Health Centre' via bhc@nsccahs.health.nsw.gov.au
- NSW Health Kids and Families website at: www.kidsfamilies.health.nsw.gov.au/publications/youth-friendly-confidentiality-resources/

Further guidance

- Section – 5.5.2 Minors
- Youth Health Policy 2011-2016: Healthy bodies, healthy minds, vibrant futures (PD2010_073)

8 Anonymity (HPP 13)

Wherever it is **lawful and practicable**, individuals must be given the opportunity to not identify themselves when entering into transactions with or receiving health services from an organisation.

Patients may seek to obtain services anonymously in cases where sensitive issues arise, such as counselling and drug use issues, or attending sexual health clinics, or provision of general medical information about lifestyle choices. Health services may provide specific clinics to deal with these issues in an anonymous way. In this context, for a health service to treat a patient anonymously means that the health service does not retain any identifying information about the patient.

In some circumstances such as where a person may be at serious risk of harm, the patient (or police) may request anonymity. In these circumstances the use of alias, or 'disguised identity' is usually a more appropriate approach, given the duty of care and clinical safety needs for the patient. (See Section 8.3 Use of alias or 'disguised identity'.)

HPP 13 does not require services to be provided anonymously in all circumstances. Health staff need to consider both the lawfulness of such a request, and its practicability before doing so.

8.1 When providing a service anonymously may be impracticable

There may be a range of circumstances where providing services anonymously may be impracticable. For example:

- a service may require follow up. If the person does not provide details to allow this, the ongoing care may be compromised
- the care to be provided involves a multi-disciplinary team, making it difficult to provide ongoing care without a clear identification of the patient
- a patient's medical status may be compromised if a clinician cannot obtain clinical information critical to providing safe and appropriate care
- services provided to staff who are also patients of the health service.

8.2 When providing a service anonymously may be unlawful

Providing services to a person without obtaining a name may be unlawful if there is a statutory requirement to obtain identifying details, or where other requirements relating to the service involve identifying the person to whom it is provided. Some examples include:

- accessing Medicare benefits requires proper identification (for example, when accessing free care in an emergency/outpatients setting, or accessing benefits from the Pharmaceutical Benefits Scheme (PBS) with a prescription to a pharmacy)
- Department of Veterans' Affairs entitlements require the provision of actual name
- prescriptions for restricted substances must include the name of the person who will receive the drugs
- where a person has been diagnosed with certain medical conditions listed as "scheduled medical conditions" under the *Public Health Act*, the health practitioner is required to record certain details, including identity, to allow the matter to be reported to the Secretary, NSW Ministry of Health
- where a person wishes to participate in an e-Health records program (see Section 16.8 National e-Health Record).

8.3 Use of alias or 'disguised identity'

The administrative management of a patient assigned an alias (disguised identity or restricted or masked identity) is different to the administrative management of an anonymous patient (as per the criteria in Sections 8.1 and 8.2 above).

The term 'alias' is also used in some patient administration systems when referring to another name by which the patient is or has been known, e.g. maiden name, previous married name. This is not to be confused with the term 'alias' when referring to anonymity.

In this context, the term 'alias' means the same as 'disguised', 'restricted' or 'masked' identity. Different health services use different terminology and may use different methods to disguise the identity of a patient. On conclusion of the patient's episode of care, the alias details will usually be reverted back to the patient's real name. This does not occur when patients are treated anonymously (see Sections 8.1 and 8.2 above).

The health service may assign to the patient an alias, in such cases as:

- the patient is under witness protection
- the patient is under police guard/ custody
- the patient is a child at risk
- the patient is at risk from potential (unwanted) visitors such as media
- court or intervention orders apply
- following a valid request from law enforcement agencies

In special circumstances, the health service may also allow an alias to be used when the patient is a staff member, or a very important person (VIP). However, in some cases health services may choose to monitor inappropriate access to these health records rather than alias the patient's identity.

Providing the patient with an alias should be done before the commencement of any treatment and preferably before the patient's details are entered into the Patient Administration System. Consultation must occur with the senior treating clinician, and others as determined by the health service to be part of the approval process for disguising a patient's identity. There should be a local policy which provides clear guidance on the process and effectively manages any clinical risk to the patient given the potential for compromise to patient care if the patient's true identity is unknown.

Prior to agreeing to assign a patient with an alias, the patient must be advised of the following:

- how the patient's 'name' will appear in the facility's Patient Administration System (PAS), and on their identity bracelet
- that the facility may not be able to provide information about the patient in response to enquiries, including from family and friends
- that the facility may not be able to receive deliveries for the patient, such as flowers or mail
- that the patient should not disclose their presence whilst in the health care facility to any persons (except to their authorised representative or 'person to contact'), as this will compromise their request for restricted identity
- that on conclusion of the episode of care, the 'disguised' details will be reverted back to the patient's known name.

8.3.1 Witness protection patients in custody

There are special provisions for witness protection patients in custody. For details contact the Medico-Legal Coordinator, Justice Health & Forensic Mental Health Network, telephone (02) 9289 5168.

Further guidance

- PD2007_094: Client Registration Policy
- Local electronic health record user guide and procedures relating to anonymity and disguised identity by contacting the local Health Information Service.

9 Retention, security and protection (HPP 5)

HPP 5 deals with the management of personal health information while it is held by a health service. It requires that:

- the information is **kept for no longer than is necessary** for the purposes for which the information may lawfully be used
- the information is **disposed of securely**
- the information should be protected, by taking such **security safeguards** as are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse.

9.1 Retention and disposal of personal health information

HPP 5 operates subject to other lawful requirements. As public sector agencies, health services are subject to the requirements of the *State Records Act 1998*. That Act has extensive provisions as to the minimum length of time public records should be retained.

Health services should therefore refer to relevant General Disposal Authorities (GDA 17, 28, 36 and 42) issued by State Records NSW in determining how long to retain and how to dispose of health records.

Further guidance:
- PD2012_069: Health Care Records – Documentation and Management
- PD2013_033: Electronic Information Security Policy

Available from State Records NSW at www.records.nsw.gov.au

- General Disposal Authority No. 17: Public health services: Patient/Client records
- General Disposal Authority No. 28: Administrative Records
- General Disposal Authority No. 36: Imaged or microfilmed records
- General Disposal Authority No. 42: Public Health Services: general practice records

9.2 Security of personal health information

HPP 5 requires personal health information must have appropriate security safeguards to prevent unauthorised use, disclosure, loss or other misuse. What will be considered appropriate will vary depending on the way information is being stored and used.

NSW Health has a range of policies to ensure appropriate levels of security are in place, depending on the nature of the information and the way it is stored.

Further guidance
- Section 13.3 – Linkage of health records (HPP 15)
- Section 16 – Electronic health information management systems
- PD2013_033: Electronic Information Security Policy – NSW Health
- PD2009_076: Use and Management of Misuse of NSW Health Communications Systems
- NSW Premiers Circular No. M2007-04: Security of Electronic Information

9.2.1 Hard copy health records

9.2.1.1 Storage

Hard copy health records containing personal health information should be kept in lockable storage or secure access areas when not in use. Precautions, such as not storing health records containing personal health information in a public area should be taken, where practicable. Care should be taken not to leave documents containing personal health information on work benches or anywhere they may be visible or accessible to unauthorised people, including clinical areas, meeting rooms and publicly accessible areas.

9.2.1.2 Access at patient bedside:

Where practicable, health records should not be left at the patient bedside and where health records are held at the patient bedside they should be limited to what is necessary for safe patient care, for example, medication and observation charts and care plans. Detailed clinical notes and results reports such imaging and laboratory reports should always be retained securely at the Nurses' station.

Any bedside health record remains confidential. Access to these health records by the patient is only permitted with supervision by clinical staff. This is to assist staff to provide the patient with a full explanation about their health information contained in their health record and to avoid potential misunderstandings or misinterpretation arising with regards to their diagnosis and treatment.

Access to health records by family or other visitors is only permitted with supervision by clinical staff and with consent from the patient (or their authorised representative). Such consent should be documented in the health record.

If the patient, family or other visitors request further access, including copies of the health record, they should be referred to the Health Information Service (also see Section 12 Patient access and amendment (HPPs 6, 7 & 8)).

Staff should take reasonable steps to ensure it is clear that health records held at the patient's bedside are confidential and should not be accessed when clinical staff are not present. Placing a prominent notice on the front of health records held at the patient's bedside is an example of one strategy to manage privacy. See Appendix 4.3 for sample wording.

9.2.1.3 Disposal

Paper records containing personal health information should be disposed of by shredding or pulping, in accordance with the provisions of the *State Records Act*. Where large volumes of paper are involved, specialised services for the safe disposal of confidential material should be employed, and certificates of disposal obtained from the contractor.

Further guidance

- Section 9.1 – Retention and disposal of personal health information

9.2.2 Images and photography

Privacy rules only apply to personal health information where the identity of a person is reasonably ascertainable (in this case, from an image). Images referred to in this section do not include diagnostic imaging, such as x-rays or MRI scans.

Further guidance on the use of images for education or conference purposes see:

- Section 9.2.7 Training and presentations
- Section 11.2.4 Management, training or research

In certain clinical contexts, the recording of patient images may be required for the care and treatment of a patient. Some examples include:

- photographing burns, wounds, cancers, or congenital conditions to monitor response to treatment
- audio-visual recording of patients under clinical observation

It is important that the equipment used is appropriate for the purpose, for example, has the necessary level of resolution and quality to meet the clinical purpose. In relation to certain types of service situations, additional security and personal privacy issues may also arise.

For this reason, health services should consider adopting local protocols and policies. These can address these issues, including identifying the type of equipment appropriate or authorised for use in different clinical settings, and provide guidance to ensure images are captured and stored in the ongoing health record.

From time to time, emergency situations may arise where a personal device is used to capture and store images and health information for clinical use, due to the urgent need for care or treatment or advice. In such situations, staff should take particular care to transfer all data from the device to the local health records management system, in accordance with local health records management policy. The image must then be permanently deleted from the personal device.

Patient consent is not required where the capturing of images is a necessary part of diagnosis or clinical care or treatment. However, where practicable, the patient should be made aware that this is to occur, or has occurred, and the reasons why it is clinically necessary.

Staff should consult with:

- **Health Information Service** for assistance with local image management and medico-legal requirements.
- **Information Technology Department** for guidance on local image management, technical and security provisions.
- **Sexual Assault Service** with regards to images of injuries sustained by victims of sexual assault.

Photographic and audio-visual images, whether reproduced in hard copy or maintained in digital format, form a part of the patient's personal health information and as such are part of the health record. The health service must therefore provide for the secure storage, access to, use and disclosure of, these health records. The photographic image/audio-visual image should be linked to, or stored in an electronic health record system. If this is not possible, digital images should be securely stored, indexed and be easily accessible and retrievable.

The use of personal smart phones (or other personal devices) by staff to capture images of patients for non-clinical purposes is generally not permitted. The NSW Health Code of Conduct and other policies provide some guidance in this area.

Further guidance

- NSW Health Code of Conduct, Section 4 (regarding use of social media)
- NSW Government Social Media Policy & Guidelines, available at: www.advertising.nsw.gov.au/strategic-communications/social-media-policy
- Australian Medical Association: Clinical images and the use of personal mobile devices, available at: https://ama.com.au/article/clinical-images-and-use-personal-mobile-devices

9.2.3 Computer systems and applications

The Electronic Information Security Policy – NSW Health (PD2013_033) supports NSW Health in meeting its obligations for protecting personal health information.

Reference should also be made to the local security rules for computer systems and applications, including electronic health information management systems (see Section 16 Electronic health information management systems).

Staff with access to electronic applications, such as an electronic health record, may only access, view and use the system for purposes directly related to their work.

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.

If in doubt, staff should seek advice from a senior manager, local Health Information Service or Privacy Contact Officer. Staff should be provided with the appropriate level of access to physical and electronic health records (i.e. full, partial or no access) in accordance with their role and their work requirements.

Subject to the specific NSW Health policies on security of personal health information stored in an electronic environment, key privacy factors arising from HPP 5 are:

9.2.3.1 Storage

A secure physical and electronic environment should be maintained.

Further guidance

- Section 16 Electronic health information management systems

9.2.3.2 Employer-owned portable media

The storage or transfer of personal health information on portable media such as USB, CD, or laptop should be limited to employer-owned media, and should be on a temporary needs basis only. Reasonable steps must be taken when storing or transferring information in this way to reduce the risk of unauthorised access to the information, such as developing password entry into documents or systems.

For guidance on health information held on a personal device, such as a smart phone, see Section 9.2.2 – Images and photography

9.2.3.3 Disposal

Authorised disposal of health records should be done in such a way as to render them unreadable and leave them in a format from which they cannot be reconstructed in whole or in part.

Personal health information must be deleted from hardware, (including computer hard drives, printers and photocopiers) before being recycled, disposed of or sent back to a leasing agent or contractor.

Health services should ensure secure removal of the hard disk drive (HDD) from redundant PCs by designated staff. The contents should then be disposed of securely and safely by, or on behalf of, the health service. A Certificate of Destruction should be retained to confirm secure destruction.

Storage and disposal of electronic health records must be in accordance with the State Records Authority disposal and retention requirements.

Further guidance

- Section 9.1 Retention and disposal of personal health information
- Section 16 Electronic health information management systems

9.2.4 Safeguards when delivering and transmitting information

Health services should first ensure the proposed use or disclosure is authorised under HPP 10 (Use) or HPP 11 (Disclosure).

If the use or disclosure is authorised the following minimum standards should be applied when providing the information. Requirements necessary to maintain secure delivery will vary depending on the medium of transmission of the information.

9.2.4.1 Telephone

Personal health information, including admission and discharge dates, should not be given over the telephone unless it has been established that the caller has legitimate grounds to access the information and their identity can be confirmed.

- Only those authorised by the health service should give patient information by telephone. It is a matter for local determination which staff members should be so authorised.
- Personal health information should not be left on voice mail. The caller's name or the clinician's name and contact number may be provided where the patient is likely to recognise the name. Otherwise, the name of the health service may be used, if applicable.

9.2.4.2 Use of Short Message Service (SMS)

SMS may be used for communication with patients for administrative purposes, for example, to confirm an appointment, to request that the patient contacts the health service, etc.

Where patients agree to being sent their test results by SMS, health services are increasingly using SMS as a standard practice of communication with patients, including, for example, Sexual Health Services.

Even where SMS communication is standard practice, patients should, if they request it, be given other options to receive information or results.

9.2.4.3 Facsimile

Some patient information is still provided by facsimile (fax). The following steps are recommended when sending personal health information via fax:

- Fax machines used for transmission of personal health information should be secure for example, they should be located so that only authorised persons can access documents.
- Fax cover sheets should carry an appropriately worded privacy notice. See Appendix 4 for sample wording.
- The fax number should be carefully checked, and if there is any doubt as to whether the number is correct (the number may be hard to read or has not been used for a considerable time) the recipient should be contacted to confirm it.
- Store regularly used fax numbers in the fax machine's memory. Stored numbers should be checked on a regular basis to ensure they are current.
- When using a new fax number or sending to a new or unfamiliar recipient, consider telephoning the recipient prior to sending a fax.

9.2.4.4 Mail

- Packaging of mail and courier items should be secure and care should be taken that addresses are complete and correct.
- Mail should be marked 'Confidential: Attention …'
- Consideration should be made as to whether it is appropriate to use envelopes displaying the health service's details. For example, health services may wish to consider using unmarked envelopes where mail is sent to patients receiving health services which they may wish to keep confidential from other persons who may access a shared mailbox.

9.2.4.5 Transmission of electronic documents (discharge referrals/ summaries)

NSW Health has a number of systems which generate electronic documents (e.g. discharge summaries and referrals (eDRS)) to external health care providers (such as general practitioners, specialists and allied health care providers), as part of providing ongoing care in the community. These systems rely on the accuracy and currency of the providers nominated by patients to receive information. Given this, health staff should:

- check the accuracy of patient information updated in auto populated fields (including current address, GP, authorised representative) at each admission
- have processes in place to manage a consistent and single source of general practitioner, specialist and other community providers' details at the health service level
- record accurate and complete community provider details
- have processes in place to authenticate and monitor the accuracy of service provider details and to update this data on a regular and frequent basis
- provide all relevant staff with education and training on their data collection responsibilities and the importance of policies and procedures in relation to provider details
- include an appropriate privacy notice in each transmission message (see Appendix 4.2).

9.2.5 Use of email

9.2.5.1 Email within NSW HealthNet

NSW HealthNet comprises electronic transmission within NSW Ministry of Health, agencies and health services comprising NSW Health. Email within NSW HealthNet is generally secure however, staff must take care to comply with local health information policies when sending personal health information via email.

In order to provide adequate security of personal health information, the following security measures should be considered:

- Use of email should not replace the recording of personal health information in electronic or paper health care records. However, an email containing health information used for the purposes of providing treatment or ongoing healthcare is likely to constitute a health record, in which case the email should be incorporated into the patient's health record.
- The subject title of emails which include personal health information should include 'Confidential'.
- Emails which include personal health information must include patient identifiers to ensure that the content of the email, or the email itself, is filed against the correct patient. The national standard for patient identification requires that the following details are provided in all circumstances when referring to a patient: patient's name, sex, date of birth, and Medical Record Number (MRN).
- As with all use of personal health information, only include health information which you know to be required for the purpose of the email communication.
- Double check that the email address is correct. Wherever practicable, request that the recipient provides you with their email address by emailing you first.
- Take particular care not to inadvertently copy unintended recipients when sending the email.
- Exercise caution when using the 'Reply All' function. Always check that it is appropriate for the content of your email to be provided to recipients.
- Password-protection or encryption of personal health information for emails sent within NSW Health for purposes outside of patient care, for example, for health service funding, insurance or other management purposes.

For guidance on health service activities which are considered to be directly related to patient care, see Section 11.2.1 Directly related purpose.

9.2.5.2 Email external to NSW HealthNet

The NSW Health Electronic Information Security Policy states that transmission of personal health information to destinations external to NSW Health are not considered secure, and should be password-protected or encrypted prior to transmission in accordance with local health service policy.

Care should be taken to avoid including patient details in the email subject title or text. The recipient should be made aware of the password via telephone or separate email.

Emails and attachment containing personal health information should be deleted from the recipient's inbox (and trash emptied) within a reasonable timeframe.

Further guidance

- Electronic Information Security Policy (PD2013_33)
- Communications – Use & Management of Misuse of NSW Health Communications Systems (PD2009_076)

9.2.6 Printing and copying

The more copies of personal health information that exist, the more likely it is that a breach of privacy may occur or that the incorrect version will be used. For this reason health records containing personal health information should not be copied or printed unless it is essential to do so.

When printing documents containing personal health information, the person printing should personally remove the document from the printer. If personal health information is printed regularly, consideration should be given to placing a dedicated printer in a secure area. This will minimise the chances of inadvertent access by unauthorised people and counteract the danger of print jobs being lost in large print buffers.

9.2.7 Training and presentations

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.

Consideration should be given to de-identification of photos, slides and other visual aids. When identification of individuals is necessary, the consent of the patient should be obtained.

Identifiable and potentially identifiable information can be used in limited circumstances for training purposes, including those involving clinical placements, and only in compliance with NSW Privacy Commissioner's Statutory guidelines on training. Staff should also seek advice from their local Privacy Contact Officer.

Further guidance

- Section 11.2.4 – Management, training or research
- NSW Privacy Commissioner's *Statutory guidelines on training*: www.ipc.nsw.gov.au/privacy/ipc_legislation.html

9.2.8 Conversations

It is important to ensure that patient information is not discussed in public areas such as corridors or lifts or anywhere where it is likely to be overheard.

Meetings to discuss patients should not be held in coffee shops, cafeterias or other public areas.

9.2.9 Visibility of computer screens

Users should be mindful of using electronic devices that contain and display health records in public areas, and where possible, ensure that the computer screen cannot be seen by anyone other than the user.

If left unattended, the computer screen should be locked to limit access to personal health information. Screen savers and locks should be used where possible to reduce the chance of casual observation.

9.2.10 Whiteboards, patient journey boards, etc. in public view

It is common practice to display limited personal health information about patients on wards using a whiteboard, electronic board, patient journey board, and so on. The purpose for displaying patient information

in this way is to enable staff to deliver safe and efficient clinical care for patients. Displaying limited personal health information in this way enables fast and effective communication between staff.

Care must be taken to limit the display of personal health information to what is essential for this purpose, for example, to include surnames only, to exclude diagnosis, and where possible to use colours, symbols or abbreviations which are easily recognisable to staff. Clinical information should remain in the patient's health record.

The use of whiteboards, patient journey boards, etc. in public view, should be supported by written business rules to ensure appropriate use at all times, and appropriate governance to ensure compliance with privacy requirements.

Further guidance

- 'Patient Journey Boards: Balancing Clinical Benefit and Privacy Obligations', available at: www.health.nsw.gov.au/wohp/pages/patientjourney.aspx

10 Accuracy (HPP 9)

HPP 9 deals with accuracy of personal health information. It requires that personal health information must not be used without taking such steps **as are reasonable in the circumstances** to ensure that, **having regard to the purpose** for which the information is proposed to be used, the information is relevant, accurate, up to date, complete and not misleading. The importance of accuracy in health records is a critical aspect of health service provision. The health record is an essential part of treatment planning and decision making. It is important that it is accurate and up to date.

To ensure that the health record is accurate and complete:

- information should be recorded at the time of consultation or procedure, as soon as it becomes available, or as soon as it is practicable to do so
- entries should generally be made by those collecting the information or present when the information was collected
- communications between clinicians relating to care and treatment of a patient must be documented in the patient's health record, including telephone, email, SMS, Skype and any other type of communications. Where identifiable photographs or other images relating to a patient are shared between clinicians, this must also be documented in the patient's health record
- each entry should contain a clear and legible notation of the health care provider's name and designation, the date and time, and should be signed by the health care provider
- accuracy of patient details should be checked by administrative staff at each presentation, e.g. name, date of birth, address, GP details, etc., including information updated in auto populated fields
- alterations or deletions should not be made original incorrect entries should not be erased but lined through so the original entry remains readable, and such action should be explained, signed and dated
- patients should be notified of amendments to their health record where appropriate
- the treating health practitioner should periodically review the health record for correctness
- there should be an audit trail for electronic health records.

Further guidance

- Section 16 Electronic health information management systems
- PD2012_069: Health Care Records – Documentation and Management
- PD2007_094: Client Registration Policy
- Australian Standard for electronic systems AS7799

11 Using and disclosing personal health information (HPPs 10 & 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 have access to the information
- giving out summaries, or communicating the information 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. The one exception is that the disclosure provisions also allow disclosure on compassionate grounds (see Section 11.2.9), this 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 special exemption pursuant to section 62 of the *HRIP Act* is obtained. Section 15 Common privacy issues provides guidance on how to address some of these circumstances, including requests for media access (see Section 15.7) and fundraising (see Section 15.8).

It should be noted that NSW Health staff may only view, access, use and disclose personal health information when it is necessary for them to do so in order to carry out their work duties.

If a staff member is in doubt as to whether they are permitted to access, use or disclose personal health information, they should seek advice from a 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.

Example: 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, e.g. health care providers including nursing staff, anaesthetists and pathologists

Example: 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 as 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 to 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 for management, training or research purposes (see Section 11.2.4)
- use or disclosure to assist in finding a missing person (see Section 11.2.5)
- use or disclosure as part of investigating and reporting wrong conduct (see Section 11.2.6)
- use or disclosure to or by a law enforcement agency or investigative agency (see Sections 11.2.7 and 11.2.8)
- disclosure made on compassionate grounds (see Section 11.2.9).

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 &11(1)(b)

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

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. Health staff should make special efforts as are reasonable in the circumstances to explain to patients how patient information is generally used and disclosed.

Directly related 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 recognises there are activities necessary, such as provision of ongoing care, billing and following up test results which may not fall within the primary purpose for which the information was collected.

What will be 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:

- using the information to provide ongoing care to patients

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.

- 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
- 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
- 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 2012* (see Section 11.2.10 Chaplaincy services)
- sharing relevant patient information with students and other staff for training purposes (see Section 11.2.4.2 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, etc.
- using patient information for purposes relating to the operation of the NSW 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 such as monitoring, evaluating, auditing the provision of the particular product or service the health service has or is providing the person (including compliance with the NSW Patient Safety and Clinical Quality Program)
- disclosing information to an auditor or quality assessor for the purposes of monitoring, evaluating, 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 11.2.4 Management, training or research)
- using the information to investigate complaints about care provided by the health service or patient safety
- disclosing information to enable follow-up of complaints about the service or a product, or recalls of a product
- using or disclosing information to claims managers and associated persons in the course of managing
  a complaint, legal action or claim brought against the health service.

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 at the time of collection thus becomes important.

Where it is made clear to the person as part of the collection process that their information may be used or disclosed for these purposes, then there is a more persuasive argument that the person would 'reasonably expect' you 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.
- Appendix 5 – Pro Forma 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, it will be situation specific and the professional judgement of local health service staff will be required to resolve such requests. To assist staff in reaching a judgement, the following guidance is provided.

1. 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.

2. 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.

3. 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 &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

The need for a consent may arise when a third party seeks access to an individual's health record. 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 his or her health record.

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

Consent must be provided by the patient prior to a third party gaining access to a patient's health information.

Requests for access to health records by a third party may occur in a number of circumstances, for example:

- 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 the patient is deceased, it is possible that an immediate family member may be provided with access to relevant health records if they are the executor of the will or otherwise on compassionate grounds (see Section 11.2.9 Disclosure on compassionate grounds).

Where a 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 access on compassionate grounds, see Section 11.2.9.

The procedures which should be followed in such cases are set out below.

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

The consent should contain:

- full name of patient
- date of birth
- contact details (e.g. 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 the request is made for information related to an insurance or compensation claim, a 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. Patient consent is required for disclosure of additional health records.

Proof of identity

Further guidance

- Section 12.6 Obtain proof of identity

Conditions of access

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

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 & 8)
- PD2006_050: Health Records and Medical/Clinical Reports – Charging Policy
- IB2013_032: Health Records & Medical/ Clinical Reports – Rates.

11.2.2.2 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, and so would normally be obtained at admission, on commencement of the therapeutic relationship, or where there are many or complex issues the patient needs to consider before consenting.
- 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 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 is otherwise allowed under the Health Privacy Principles.

11.2.3 To prevent a serious and imminent threat to health or welfare HPP 10&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 colleagues or a senior health practitioner before acting.

Example: A patient of a community health service arrives in an agitated state, making threats against a close family member over a custody dispute, and leaves. 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 and imminent risk, and so could disclose the information in order to address this risk.

Example: A Public Health Unit conducting an investigation 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.

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, etc.), and when the patient poses a threat to themselves or any individual including staff, or to public health or public safety. Key principles to managing violent behaviour are:

1. Privacy obligations must be balanced with health service's obligations to ensure a safe workplace under the *Work Health and Safety Act 2011*.

2. 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.

3. When sharing information about a patient, focus on patient behaviours that may pose a threat or risk, and appropriate patient management strategies.

4. A health service must take reasonable steps to ensure the information they share is accurate, relevant, up to date, complete and not misleading.

5. Use patient alerts or patient flagging in accordance with *'Zero Tolerance: Response to violence in NSW Health workplace'*.

Further guidance

- PD2005_315: Zero Tolerance: Response to violence in NSW Health workplace
- PD2005_409: NSW Health Workplace Health and Safety – Policy and Better Practice Guide
- PD2005_339: Protecting People and Property: NSW Health Policy and Guidelines for Security Risk Management in Health Facilities

Contact: Workplace Relations Branch, NSW Ministry of Health

11.2.3.3 Public Health Act 2010 – Notification of public health risk

The *Public Health Act* 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, AIDS 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 co- ordinator, or the HIV and STI (Sexually Transmissible Infections) Branch, NSW Ministry of Health.

See Section 4.1.3.2 HIV/AIDS-related information, for information on the *Public Health Act* limitations imposed on the disclosure of information indicating a person's HIV status, and information that a person has undergone an HIV test.

Further guidance

- Section 15.9.6 Managing public health risks
- PD2005_184: Contact Tracing Guidelines for Sexually Transmissible Diseases and Blood Borne Viruses
- PD2009_023: HIV – Management of People with HIV Who Risk Infecting Others
- PD2005_068: Tuberculosis Management of People Knowingly Placing Others at Risk of Infection
- PD2005_162: Health Care Workers Infected

11.2.3.4 Genetic information

Since 2014, the HRIP Act has included provisions and processes for genetic information, which 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 & 11(1)(c1) genetic information can be used and disclosed where:

i. The disclosure is to a genetic relative of the individual to whom the genetic information relates, and

ii. 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

iii. The disclosure is made in accordance with guidelines, if any, issued by the NSW Privacy Commissioner for the purposes of this paragraph.

The NSW Privacy Commissioner has issued guidelines entitled "Use and disclosure of genetic information to a patient's genetic relatives: Guidelines for organisations in NSW" available at: www.ipc.nsw.gov.au/

The Guidelines reflect similar guidelines already issued under Federal Privacy Law. They encourage health practitioners to take all reasonable steps to obtain consent from the patient (or 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 authorised representative (such as the executor of the deceased person's estate) has refused to consent on behalf of the patient, and the genetic relative 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 11.2.9 Disclosure on compassionate grounds).

It should be noted that the scope of the Guidelines does not include situations concerning genetic information that present 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

- IB2014_065: Information & Privacy Commission Guideline: Use & disclosure of genetic information without consent
- Section 11.2.9 Disclosure on compassionate grounds

11.2.4 Management, training or research HPPs 10 & 11 (1) (d), (e) & (f)

A health service may use or disclose personal health information if this 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.

11.2.4.1 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. Each of the exceptions 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. De-identified information cannot be re-identified.

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 '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.

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.

11.2.4.2 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 Statutory guidelines, go to:
www.ipc.nsw.gov.au/privacy/ipc_legislation.html

Management guidelines

The management guidelines discuss each of the preconditions in detail, and draws attention to the relevant "directly related purpose" which may otherwise apply. The guidelines then provide for a Human Research Ethics Committee to consider the proposed use or disclosure and assess whether, on balance it is in the public interest.

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 (Commonwealth)*. 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 where de-identification would defeat the purpose of the training. The guidelines then set requirements for managing such training.

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

Also see Section 9.2.7 Training and presentations.

Clinical placements and students

Student health professionals must sign a Privacy undertaking (see Appendix 3), and must comply with privacy law and all NSW Health policies.

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.

Further guidance

- To view the Statutory guidelines, go to www.ipc.nsw.gov.au/privacy/ipc_legislation.html
- PD2012_051: Disclosure of Unit Record Data held in NSW Ministry of Health Data Collections for the Purposes of Research or Management of Health Services

11.2.5 Finding a missing person

HPPs 10(1)(g) & 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.

11.2.6 Investigating and reporting wrong conduct HPP 10(1)(h) & 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:

- information to be provided to the Health Care Complaints Commission or a NSW Health Professional Council or National Board
- information to be provided to units of the NSW Health department which may conduct investigations into breaches of legislation, including the Pharmaceutical Services Unit (NSW Ministry of Health)
- information to be shared between these investigative units within NSW Health.

11.2.6.1 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 2004*. 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 2004* and should be referred to the PID co-ordinator or Chief Executive for consideration.

Further guidance
PD2011_061: Public Interest Disclosures

11.2.7 Law enforcement agencies, including police HPPs 10(1)(i) &11 (1)(j)

HPP's 10 and 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 are reasonable grounds to believe that an **offence may have been or may be committed**.

11.2.7.1 What is a "law enforcement agency?"

The *HRIP Act* 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
- Juvenile Justice NSW

11.2.7.2 What sort of information can be provided?

The law enforcement exemption under HPP's 10 and 11 is very broad. It covers any information relating to an offence which has or may be committed, provided that 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 'Identifying and Responding to Domestic Violence' 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 there is an immediate risk to public safety or health staff are threatened.

If after considering these matters, 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.

Any other 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

11.2.7.3 Certificate of expert evidence

Evidence in legal proceedings is normally provided verbally, however, under certain circumstances, expert opinions or technical evidence may be given in a court proceeding without requiring the expert or technician to attend the proceedings as a witness. The *Evidence Act 1995* allows for this to be done through providing a 'certificate of expert evidence'.

The certificate of expert evidence cannot be provided without the consent of the patient to whom the certificate relates.

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 11.2.7.2 What sort of information can be provided?).

11.2.7.4 How should requests from law enforcement agencies be handled?

Requests should be in writing on letterhead (or electronic equivalent), 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
- Where clinical information is necessary, this should be limited to a general outline of the patient's condition and/or injuries.

Example: A paramedic attends a male 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 they are competent to be interviewed.

11.2.7.5 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 11.2.7.2.

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' and is available from the Emergency Care Institute website at: www.ecinsw.com.au/clinical-support-tools

Other circumstances recognised by the *HRIP Act* 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 11.2.5)

Further guidance

- Section 11.2.7.2 – What sort of information can be provided?
- Section 11.2.3 – To prevent a serious and imminent threat to health or welfare
- Section 11.2.5 – Finding a missing person
- Section 11.3.4 – Reporting "serious criminal offences"
- Section 11.3.6 – Search warrants and subpoenas
- Section 15.2 – Requests from state and federal police

11.2.8 Investigative agencies HPP (10)(1)(j) & HPP (11)(1)(k)

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
- the Police Integrity Commission, the Inspector of the Police Integrity Commission and any staff of the Inspector
- the Health Care Complaints Commission
- the Office of Legal Services Commissioner

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.

11.2.9 Disclosure on compassionate grounds HPP 11(1)(g)

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 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 **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.

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.

Disclosure on compassionate grounds would not generally cover release of an individual's entire health record.

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* or the *Government Information (Public Access) Act* (see Section 12 Patient access and amendment (HPPs 6, 7 & 8)), or otherwise to issue a subpoena via their legal representative.

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.

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.

Example: 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.

Example: A person has died suddenly at hospital without indicating his views 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.

Example: 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.

11.2.10 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 & 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 views are complied with.

Further guidance

- NSW Health & Civil Chaplaincies Advisory Committee NSW Memorandum of Understanding (PD2011_004)
- NSW Health Chaplaincy Services and Privacy Law (IB2008_044)
- NSW Health Privacy Leaflet for Patients – see Appendix 5

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 that is required by the authority, no more and no less
- 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.

The *Poisons and Therapeutic Goods Act 1966*, section 42, 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* 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 Child Protection and Violence Prevention website: www.kidsfamilies.health.nsw.gov.au/current-work/child-protection-and-violence-prevention
- NSW Health Policy Directive: Child Wellbeing and Child Protection Policies and Procedures for NSW Health (PD2013_007)
- Child Wellbeing and Child Protection – NSW Interagency Guidelines: www.community.nsw.gov.au/kts/guidelines/info_exchange/introduction.htm
- NSW Interagency Keep Them Safe website and Mandatory Reporter Guide: www.keepthemsafe.nsw.gov.au/

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*.

Chapter 16A provides for certain agencies, generally those working with children and families classed as "prescribed bodies" under the *Care Act,* to exchange information with other prescribed bodies relating to a child or young person's safety, welfare or wellbeing in certain circumstances. Under Chapter 16A, information relating to the safety, welfare or wellbeing of a child or young person 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 or persons) that might arise in the recipient's capacity as an employer.

A prescribed body includes:

- the NSW Police Force
- a NSW government department or NSW public authority, including Family and Community Services (FACS)
- a NSW government school or a NSW registered non-government school
- a NSW TAFE
- a NSW public health organisation (PHO) or a NSW licensed private health facility
- a FACS-accredited or FACS–registered out-of-home care agency
- a FACS-accredited adoption service
- the Family Court of Australia, the Federal Magistrate's Court of Australia, "Centrelink" and the Department of Immigration and Border Protection and
- 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.

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

- PD2013_007: *Child Wellbeing and Child Protection Policies and Procedures for NSW Health*

Section 248

Section 248 of the *Care Act* allows for the exchange of information relating to the safety, welfare and wellbeing of a child or young person between prescribed bodies.

While generally FACS will use Chapter 16A to request information relating to child protection, in some situations FACS 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.

11.3.2.1 Reporting children and young people at risk of significant harm

Under section 24 of the *Care Act,* 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 FACS.

Under section 27 of the *Care Act,* health staff must make child protection reports to FACS where they have reasonable grounds to suspect that a child or young person is at risk of significant harm to FACS, or to the NSW Health Child Wellbeing Unit Under section 27A.

Under section 25 of the *Care Act,* 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 FACS.

Reference to the NSW Mandatory Reporter Guide may assist in ascertaining whether the staff member's child protection concerns meet the threshold of 'risk of significant harm'.

See NSW Mandatory Reporter Guide at: www.keepthemsafe.nsw.gov.au/

11.3.2.2 Protection for mandatory reporters

Section 29 of the *Care Act* provides for the protection of persons who make reports or provide certain information to Family and Community Services (FACS) or to the NSW Health Child Wellbeing Unit.

Where access is being requested to reports made to FACS, 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 FACS, 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 *Care Act*, a written report of the examination may be disclosed to the Family and Community Services 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 *Care Act* from legal action in relation to allegations of professional misconduct and defamation.

11.3.2.4 Child Sexual Assault Investigation Kit Records

The Child Sexual Assault Investigation Kit (SAIK) includes consent to disclose SAIK records to FACs and Police for medico-legal purposes. Chapter 16A of the *Care Act* 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 where the request meets the requirements of Chapter 16A of the *Care Act*. 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.

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 alleged 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:

- NSW Health Policy Directive: Child Wellbeing and Child Protection Policies and Procedures for NSW Health (PD2013_007)
- Child Wellbeing and Child Protection – NSW Interagency Guidelines www.community.nsw.gov.au/kts/guidelines/info_exchange/introduction.htm
- NSW Interagency Keep Them Safe website and Mandatory Reporter Guide www.keepthemsafe.nsw.gov.au/
- NSW Health Child Protection and Violence Prevention website: www.kidsfamilies.health.nsw.gov.au/current-work/child-protection-and-violence-prevention

Contact:

- **NSW Kids and Families on telephone (02) 9391 9000**
  www.kidsfamilies.health.nsw.gov.au/

- **NSW Health Child Wellbeing Unit on telephone 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 Access to health records of correctional centre inmates

Sharing of information between Justice Health & Forensic Mental Health Network and the Corrective Services NSW is detailed in 'Guidelines on the use and disclosure of inmate/patient medical records and other health information'.

The staff of Justice Health & Forensic Mental Health Network may disclose information relating to the medical history of an inmate to Corrective Services NSW, or other correctional facilities, to investigate an incident or assault involving that inmate. Requests should be in writing indicating the basis for disclosure. Consent from the inmate/patient must be obtained, unless other lawful disclosure applies (for example, risk of harm, see Section 11.2.3, or law enforcement, see Section 11.2.7).

Further guidance

- 'Guidelines on the use and disclosure of inmate/patient medical records and other health information' available at:
  www.justicehealth.nsw.gov.au/publications/guidelines-disclosure-medical-records.pdf
- IB2010_044: *Mental Health Information and the Health Records and Information Privacy Act 2002*

11.3.4 Reporting "serious criminal 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 an offender. 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 two 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 possession offences or any offences under public health legislation.

The Regulations under the *Crimes Act* also provide that prosecution for an offence under this law will not be commenced against a person without the approval of the Attorney General if the information was obtained in the course of practising as a:

- health practitioner,
- psychologist,
- nurse,
- social worker, including, a support worker for victims of crime, and a counsellor who treats persons for emotional or psychological conditions suffered by them,
- researcher for professional or academic purposes.

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.

Further guidance

- Section 11.2.7 Disclosure of information to law enforcement agencies, including police
- NSW Health Policy Directive: Domestic violence – identifying and responding (PD2006_084)
- Interagency guidelines for responding to adult victims of sexual assault, issued by NSW Health, the NSW Police Force and the Director of Public Prosecutions. The guidelines are available to NSW Health staff by contacting their local Sexual Assault Service.
- Interagency guidelines for responding to domestic violence: It Stops Here: Safer Pathway, and Domestic Violence Information Sharing Protocol, available at:
  www.domesticviolence.nsw.gov.au/services

11.3.5 Coroner

The *Coroners Act 2009* requires notification to the Coroner of deaths occurring under certain conditions. The Coroner will require original health records. 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 order that the pathologist or medical officer conducting the postmortem may access the health record. When health records are tendered to the Coroner, the treating health practitioner should be notified.

Where a request or an order is made by the Coroner, or the police for coronial purposes, it should be received on letterhead (or electronic equivalent), with reference to section 53 of *the Coroners Act*, and detailing which information is required.

Further guidance

- PD2010_054: Coroners Cases and the Coroners Act 2009

11.3.6 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, he or she 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, i.e. 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.

Further guidance

- PD2010_065: Subpoenas

11.3.7 Health Care Complaints Commission

11.3.7.1 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.

11.3.7.2 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.

11.3.8 The Ombudsman

The Ombudsman is empowered to require health authorities to supply information where a formal investigation is being conducted under the *Ombudsman's Act 1974*.

11.3.9 Official visitors

Official visitors are appointed under the NSW *Mental Health Act 2007* to inspect declared mental health facilities.

Under Section 132 of the Act, official visitors must be provided with access to health records relevant to the care of patients.

11.3.10 Child Death Review Team

Chapter 9A of the *Coroner's Act 2009* provides for a Domestic Violence Death Review Team, which includes a Child Death Review Team.

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.

11.3.11 Workcover

Relevant sections of the *Work Health and Safety Act 2011*, allow inspectors from Workcover 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* 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

11.3.12 Commonwealth Agencies

11.3.12.1 Commonwealth Department of Family and Community Services

The Commonwealth Department of Family and Community Services has powers under the *Social Security (Administration) Act 1999 (Commonwealth)* 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.

11.3.12.2 Veterans' Affairs

Under Section 128 of the *Veterans' Entitlement Act,* 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.

Disclosure of patient information for purposes other than funding are subject to the exemptions listed in Section 11.2.

Deaths of repatriation patients must also be reported to the Department of Veterans' Affairs.

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.

11.3.12.3 Immigration and border protection

The Commonwealth Department of Immigration and Border Protection has powers under section 18 of the *Migration Act 1958 (Commonwealth)* to obtain information about illegal non-citizens.

The power allows the Department of Immigration and Border Protection 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.

11.3.13 Statutory reporting requirements

The public health system is required by legislation to notify authorised agencies of certain types of personal health information.

Public Health Act 2010

The following must be reported to the NSW Ministry of Health:

- Scheduled Medical Conditions
- Inpatient statistics
- Maternal and perinatal data for Perinatal Data Collection
- Cancer cases (through the NSW Cancer Registry)
- Register for Congenital Conditions

Further guidance

- Section 15.9.6 Managing public health risks
- PD2005_210: Inpatient Statistics Collection (ISC)
- PD2009_012: Cancer Registry – Notifying Cancer Cases to the NSW Central Cancer Registry
- PD2012_055: Congenital Conditions Register – Reporting Requirements
- IB2012_011: Notification of Infectious Diseases under the NSW *Public Health Act*
- PD2012_047: Notifiable Conditions Data Security and Confidentiality

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 registration board.

Births, Deaths and Marriages Registration Act 1995

- Perinatal deaths must be reported to the Principal Registrar.

Health Services Act 1997, Private Hospitals and Day Procedure Centres Act 1988

- Adverse drug reactions must be reported to the Australian Drug Evaluation Committee at the Ministry
  of Health.

Home and Community Care Act 1985 (Commonwealth)

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* 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

- PD2008_050: Home and Community Care Minimum Data Set Version 2 – Collection & Reporting Requirements

11.3.14 *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 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 website at: www.health.nsw.gov.au/pharmaceutical

11.3.15 Information required by the Minister or Premier

NSW privacy laws also recognise that from time to time the executive arm of government (i.e. 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.

11.3.15.1 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.

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).

12 Patient access and amendment (HPPs 6, 7 & 8)

12.1 Access to personal health information (HPPs 6 & 7)

The *HRIP Act* allows a person to apply for access to information a health service holds about them.

- **HPP 6** requires a health service to take reasonable steps to allow a person to ascertain if the service holds information about them.
- **HPP 7** establishes a right to apply for access to that information.

Health services are required to inform patients of these options at the time information is collected (see Section 7 Collecting personal health information (HPPs 1-4)).

12.2 *Interaction of HRIP Act and Government Information (Public Access) Act 2009 (GIPA Act)*

The general principle under both privacy and *GIPA Act* laws is that **a person will be presumed to have a right to access the information an organisation holds about them**. This also reflects NSW Health policy since at least 1989.

The *GIPA Act* provides any person with a right to apply for access to information held by NSW government agencies, including personal and health information. Access to personal health information is through "formal access". The Act establishes four ways for the public to access government information:

1. **Mandatory Disclosure**
NSW Health agencies must disclose certain information, known as open access information, unless there is an overriding public interest against disclosure. It is unlikely that mandatory disclosure would include personal health information. In most cases, open access information must be available on the agency's website.

2. **Informal Release**
Agencies are encouraged to release information without the need for a formal application, unless there are good reasons to require one.

3. **Proactive Release**
Agencies are encouraged to release as much information as possible free of charge or at the lowest reasonable cost.

4. **Formal Access**
If information cannot be accessed as above, a formal access application may be necessary.

In practice, NSW Health agencies generally process applications for health information under the *HRIP Act* as this is a less onerous process for both the agency and the applicant. Where an individual specifically asks for their application for access to health information under the *GIPA Act*, this can and should be done.

Refer to local Health Information Service for advice on local processes for access under the *HRIP* and *GIPA Acts*. See Section 4.2.2 *Government Information (Public Access) Act 2009*

12.3 Where access is refused

The *HRIP Act* recognises that sometimes circumstances will arise where access may be refused. This is most often likely to arise where access may place the person seeking their information, or another person, at risk of harm. HPP 7 therefore allows refusal of access if a refusal "is authorised or allowed under a law".

This provision is designed to recognise circumstances where access could be refused under the *GIPA Act*. If access can be refused on this basis under the *GIPA Act*, the health service will be "lawfully authorised" to refuse access under the *HRIP Act*. However, in such circumstances, decision making should be clearly documented, including in which circumstances access will not be granted, which considerations were made to determine whether to disclose or not disclose certain information, and the professional status of the person who has made that decision.

There may also be other grounds for refusal in the *GIPA Act*. Staff should refer any enquiries to their local GIPAA Right to Information Co-ordinator.

Prior to refusing access to personal health information, staff should consult with the Privacy Contact Officer for their agency.

12.3.1 Reasons for refusing access

The *HRIP Act* access provisions focus on individuals accessing their own medical and health information. As such, it will be rare to refuse access.

Whilst a person is presumed to have the right to access information about them (or the person they represent), the *GIPA Act* requires an agency to consider whether it is in the public interest to disclose the information.

The most common circumstances where access may be refused for public interest reasons under the *GIPA Act*, and therefore also under the *HRIP Act*, are set out in the *GIPA Act* (see section 14, Table 3 of the Act), and are provided below.

12.3.1.1 The disclosure of information could reasonably be expected to reveal another individual's personal information

Prior to providing access to a record, care must be taken to assess the record and identify any personal or personal health information which does not relate to the patient. This is sometimes referred to as 'third party' information.

In some circumstances, it will be reasonable to provide access to third party information, such as:

- where this information is already known to the patient,
- where the third party has provided their consent,
- where there is no reason for the health service to believe that disclosure of the third party information would unreasonably reveal another individual's personal information.

In other circumstances, it will be necessary to withhold either all of the third party information, or part thereof.

Consideration must be given as to whether it would be unreasonable to disclose all or part of the third party information, given certain factors including:

- whether disclosure of the third party information could endanger the life or physical safety of any person,
- whether disclosure of the third party information may reveal the personal health information of any person (including details such as Hepatitis C or HIV status),

- whether disclosure of the third party information relates to views, events or circumstances which the patient, or the person seeking access, may not be aware of, and it would be unreasonable in the circumstances to disclose this information.

Carer details

Health records may contain details about the patient's carer, particularly records relating to children and young people in out-of-home-care, people with a disability and the elderly. Care must be taken not to disclose carer details where it is not evident that this information is already known to the patient, or person acting on behalf of the patient.

Staff details

The names of staff included in a health record is generally not considered 'personal information' and can be disclosed, unless:

- disclosure could reasonably be expected to expose the staff member to a risk of harm,
- other privileges apply, such as in the case of a report to Family and Community Services (FACS), where all references to the staff 'reporter' are to be removed, including previous or subsequent entries made in the health record of their name or designation. Other notations of a report being made should also be removed.

Some examples of where third party information contained within a record may be withheld (redacted) are provided below.

Example 1: A health record about a young person contains personal health information about their parent's mental health at the time of their birth about which the young person may not be aware. As the young person's health record contains third party information, this may only be provided with the parent's consent, even though it is part of the young person's health record. An alternative would be if consent is absent, all references to third party information must be blacked out (redacted) prior to access being provided to the young person.

Example 2: A patient of a sexual health service gives a detailed history about his exposure to HIV which includes details about his partner's sexual health and HIV positive status. As this patient's health record contains third party information, subject to additional protections under the Public Health Act, care must be taken around its release. In circumstances where the third party, (in this case, the partner) has not consented to the release of their personal health information in relation to their HIV status or other sexual history, all references to third party information must be blacked out (redacted) prior to any access being provided to the health record.

12.3.1.2 The disclosure of information could reasonably be expected to expose a person to a risk of harm

Care must be taken to identify whether the release of information may have an adverse impact on the physical or mental health of the applicant, or any other person, including a child, staff members, etc.

In rare circumstances where the treating health practitioner considers access could be prejudicial to the physical or mental health of the patient or to another person, the health record may be referred to a third party such as an independent health practitioner for assessment. If this occurs, the health record plus the assessment should then be referred to the Department Head or Director of Medical Services for review and a decision made as to whether the applicant should be granted access to all or part of the health record. In some cases it may be necessary for access to be provided via a health practitioner nominated by the applicant.

Where it is determined that access provides no risk or minimal risk to the physical or mental health of an individual, but there remains a concern as to the impact the information may have on the applicant, a written explanation to this effect should be given to the applicant encouraging them to seek advice from a health practitioner if they have any concerns or questions. A copy of this should be retained on the health record.

Where it is determined that access will not be granted under the *HRIP Act*, then reference should be made to section 14 of the *GIPA Act* (see Section 12.4 Providing access). Consideration should then be given to the public interest considerations against disclosure and/or whether conditions should be placed on the release of the health information.

12.3.1.3 The disclosure of personal information about a child would not be in the best interests of the child

When access is sought to information relating to a child and there are concerns that disclosure may adversely affect the child, a senior health practitioner should carefully review the health record to determine whether disclosure is in the best interests of the child.

Example: The child's parents are separated. The child lives with her mother but sees her father on alternate weekends. There are no parenting orders in place and each parent is entitled to seek access to the child's health record. The child's relationship with her father has been strained but is improving and to this end she has been seeing a community social worker. Her father has sought access to these counselling records and the clinicians are concerned that the child's progress (and her relationship with her father) will deteriorate if he has access to these health records. The clinicians may rely upon the public interest considerations against disclosure in the GIPA Act, section 14, to refuse the father's access to these health records, namely, that the disclosure of personal information about the child would not be in the best interests of the child (see the GIPA Act, Table at 3(g)). The clinicians will also need to provide the father with a reason for this decision, as it is not sufficient to only quote the legislation. Guidance can be sought from the Legal & Regulatory Services Branch.

12.3.1.4 The disclosure of information could reasonably be expected to contravene an Information Protection Principle under the Privacy and Personal Information Protection Act 1998, or a Health Privacy Principle under the Health Records and Information Privacy Act 2002

When providing access to information, care must be taken not to breach the privacy principles. Important principles to be mindful of when processing a request for access are:

- Take reasonable steps to maintain the **security** of health records, and protect health records from unauthorised access, use, modification and loss. For example, an applicant should not be left alone with the original health record during access.
- Take reasonable steps to maintain the accuracy and completeness of health records, ensuring that information is relevant, accurate, up-to-date, complete and not misleading. For example, if an individual's health record is stored in different formats (electronic and paper) and/or different locations, ensure the applicant is provided with access to all relevant information, following assessment.
- Be mindful that access to health information can only be provided with the **consent** of the individual to whom it relates, or their authorised representative.

Note: Personal health information may also be released in accordance with Health Privacy Principles 10 and 11 (see Section 11 Using & disclosing personal health information (HPPs 10 & 11)).

12.4 Providing access

Where access is granted, it can be provided in the following manner:

- electronic or paper copy
- direct access, by supervised viewing of the health record on the health service's premises. A health practitioner or health information manager must always supervise access to health records. Patients may request the assistance of a health practitioner in interpreting the health record.
- a copy sent to a health practitioner nominated by the applicant as allowed for in the *GIPA Act*, Section 73(3), which states:

A condition may *be imposed that access to medical or psychiatric information will only be provided to a* health *practitioner nominated by the applicant and not to the applicant personally."*
It is at the discretion of the health service to determine whether this is necessary, for example:

i. where there is a risk of harm to the applicant or any other person or child, which could be avoided if access is provided via a health practitioner
ii. where the applicant has requested access via a health practitioner.

- copies sent to a third party, such as an insurance company, solicitor, or legal representative. This should only occur where the third party clearly acts for the applicant or has made the application on his or her behalf and has provided a written consent from the patient.

In all cases, care must be taken to only release the information which is requested. In the case of a subpoena, this will be listed in the Schedule. See Section 11.3.6 Search warrants and subpoenas.

The requirements for application imposed on access by patients mirror the requirements imposed on other third party access. See Section 11.2.2.1 Where a third party seeks access.

Copies of health records may also be provided to family members on compassionate grounds. See Section 11.2.9 Disclosure on compassionate grounds.

12.5 Other conditions of access

12.5.1 Parenting orders

Where a request is made from a parent in circumstances of divorce or separation, consideration should be given to the terms of any parenting order issued by the Family Court. Parenting orders set out the responsibilities and role of each parent.

Where there is no parenting order, both parents will retain parental responsibility for the children, and therefore have a right of access to the health record.

One parent's request for the other parent not to access the child's health record cannot of itself be a basis to refuse access, unless there are reasonable grounds to believe that this access would put the child, or another person, at risk of harm. See Section 11.3.2. Child protection.

12.5.2 Apprehended Violence Order

Where there is an Apprehended Violence Order (AVO)* against a parent, this does not affect their right to ***apply*** for access to health information relating to their child. As with all applications, care should be taken not to disclose personal details, such as address details, personal or health information about a third party which may be included in the child's health records.

**This includes both an Apprehended Domestic Violence Order (ADVO) and an Apprehended Personal Violence Order (APVO).*

12.5.3 Reports to Family and Community Services (FACS)

The *Children and Young Persons (Care and Protection) Act 1998*, section 29 provides for the protection of persons who make reports or provide certain information to Family and Community Services (FACS).

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

Further guidance

- Section 11.3.2 Child protection

12.5.4 Access by staff responding to a complaint, claim or investigation

When a staff member, including Visiting Medical Officer or Medical Officer, seeks access to health records to respond to a complaint made about them or the care they provided, it is appropriate in most cases that they be provided with access to relevant health records to enable them to respond to the complaint, claim or investigation, without the need to seek consent from the patient.

This is usually achieved by providing the staff member with supervised access to the health records at the relevant health care facility. However, in some cases the staff member may need to spend more time reviewing the health record and it is reasonable that they are provided with a copy of the relevant parts of the health record. Access may normally also be provided where the staff member is no longer involved in providing treatment to the patient.

Alternatively, relevant health records may be provided to the staff member's solicitor, and this may be required where the staff member is no longer employed by the organisation. Before releasing health records to a solicitor, the health service should first obtain written confirmation from the solicitor that they act on behalf of the staff member.

In releasing any of this material to either a solicitor or a VMO/MO, health services should reiterate their privacy obligations with respect to the health records. For example, health services should include wording to the effect of:

> *"Information relating to [XXX patient] is provided to you to assist you in responding to a [complaint/claim/investigation] regarding your conduct. You are required, in accordance with privacy laws, to keep this information confidential and to only use it for the purpose of responding to the current [complaint/claim/investigation]."*

In the case where a staff member is responding to a claim of professional misconduct, where appropriate, a staff member may be permitted to view relevant medical records. This would most likely occur under supervision and at the discretion of the investigator.

In rare circumstances, it may be inappropriate to provide a staff member with access to health records, for example, where there are reasonable grounds to believe that providing access may present a risk of harm to any person(s), or where access could compromise legal proceedings. Legal advice should be sought in such instances.

Further guidance

- Section 11.2.1 Directly related purpose
- Section 11.2.2 Consent
- Section 15.6 Legal claims and insurance

12.6 Obtain proof of identity

When seeking access to personal health information, as a minimum an applicant must provide proof of identity in the form of a certified copy of any one of the following documents:

- Current Australian driver's licence
- Current Australian passport

- Other proof of signature and current address details (2 proofs of identity may be required in this case).

In addition to the above minimum requirement, a health service may require further proof(s) of identity at their discretion.

If applying by mail, certified photocopies of identification can be accepted.

A certified copy requires the signature and authorisation by a Justice of the Peace (JP) or solicitor to certify that it is a true copy of the original document.

12.7 Fees and charges

HPP 7 requires that a health service provides access to health information without excessive expense.

For guidance on fees and charges for access to health information, health services should refer to the NSW Health policy on fees and charges for access to health records.

Further guidance

- PD2006_050: Health Records and Medical/ Clinical Reports – Charging Policy

12.8 Additions and corrections (HPP 8)

HPP 8 allows individuals to request a health service to make appropriate amendments to their personal health information.

HPP 8 provides that an amendment can be requested to ensure:

- the information is accurate
- the information is relevant, up to date, complete and not misleading, taking into account the purpose for which the information is collected and used.

Health services should not alter a health record unless of the view that it is necessary to do so in line with the above criteria.

The request for amendment should be retained in the patient's health record.

Patients should be notified of the outcome of their request for amendment, and if amendment is refused, the reason for the refusal.

12.8.1 Where an alteration is included

Untraceable alterations or deletions to clinical information held in the health record should not be made. Original incorrect entries should not be erased but lined through, or otherwise appropriately amended to reflect the correct information, so the original entry remains retrievable and readable.

Electronic record systems will automatically record a history of alterations and deletion, including meta data relating to date, time, and user details.

The reason for the amendment should be noted in the health record, dated and signed.

Nothing in these provisions should be taken to prevent the routine updating of demographic information, such as address, contact details and patient's general practitioner details.

12.8.2 Where an alteration is refused

If the changes requested by the patient (or other authorised party) do not meet the requirements of accuracy, completeness, etc. as set out in **HPP 8(1),** the health service is required in **HPP 8(2)** to **take such steps as are reasonable** to attach additional information as an addendum to the health record. In addition, the patient's own comments should be attached as an addendum to the health record on request, along with an explanation of the circumstances.

13 Miscellaneous (HPPs 12, 14 & 15)

13.1 Identifiers (HPP 12)

Identifiers are used by health services to uniquely identify an individual and their health records. A number of identifiers are used within NSW Health, for example:

- Medical Record Number (MRN) – an identifier used by the hospital or facility to identify a patient and his or her health record.
- Area Unique Identifier (AUID) – an identifier generated for a patient within a Local Health District.
- Enterprise Unique Identifier (EUID) – a state health identifier for a patient provided by the State Enterprise Patient Registry system.
- Individual Health Identifier (IHI) – a national identifier for a consumer provided by the National Health Identifier Service.

While identifiers may not use a person's name and address, they are designed to be unique to a specific individual and hence may be "personal health information", and subject to the privacy laws.

HPP 12 states that a health service may only assign identifiers to individuals if this is **"reasonably necessary"** to carry out any of the health services functions efficiently. All eHealth systems used by NSW Health will automatically assign a unique identifier when collecting health information for inclusion in an individual's electronic health record.

In practice, identifiers are assigned to nearly all individuals who receive services from NSW Health. The exception may be health services which do not require follow up treatment.

HPP 12 also places limits on when a private sector agency may use or disclose an identifier assigned by a public sector agency. The primary restriction is that a private organisation may only use a public sector identifier **as its own** where:

- the individual concerned has consented to this
- the use of the identifier in this way is required or authorised by or under law.

HPP 12 also outlines the circumstances where a private sector organisation can use and disclose a public sector identifier. These generally relate to situations where some of the "use" (HPP 10) and "disclosure" (HPP 11) exemptions arise.

13.2 Transferring personal health information out of NSW (HPP 14)

Health services frequently need to transfer personal health information to agencies and health services in other states and territories, as well as to the Commonwealth. This may be for care or treatment purposes, or as part of the Commonwealth-State reporting obligations.

Where a health service wishes to provide information to a body outside NSW, it must comply with both HPP 11 (disclosure) and HPP 14.

HPP 14 regulates when NSW health services can transfer personal health information to an agency outside New South Wales, establishing a list of circumstances when this will be authorised.

The most useful likely provision to rely on will be where the health service reasonably believes that the recipient of the information is subject to a law, binding scheme or contract that effectively upholds principles for fair handling of the information that are substantially similar to the Health Privacy Principles, or where the patient consents to the disclosure.

13.2.1 Within Australia

The current status of privacy policy or law means that sharing of information with health services in Australia can occur without consideration of the exceptions listed for HPP 14, noting that:

- The private sector is covered by the *Privacy Act 1988* (Commonwealth)
- All states and territories in Australia either have equivalent privacy laws or binding public sector policies across their respective systems.

13.2.2 Outside Australia

- Countries in the European Union are bound by the European Union (EU) Data Protection Directive, Directive 95/46/EC. As such, disclosure to these countries would comply with HPP 14
- In the United States of America, health information is protected under the *Health Insurance Portability and Accountability Act 1996* (HIPAA) therefore disclosure to anyone in the USA would comply with HPP 14

In relation to other external jurisdictions health services should:

First, seek information from the recipient as to whether there are equivalent privacy laws and if not:

Second, consider whether any of the other exemptions listed in HPP 14(2) apply. These cover:

- **Consent** – the individual to whom the information relates consents to the transfer
- **Contractual obligation** – the transfer is necessary for the performance of a contract between the individual and the health service
- **Benefit to the individual** – the transfer is for the benefit of the individual, and it is impracticable to obtain their consent, and if it were practicable to obtain such consent, the individual would be likely to give it
- **To prevent serious threat to individual or public health** – the transfer is reasonably believed to be 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 (see Section 11.2.3)
- **Reasonable steps** – the health service has taken reasonable steps to ensure that the information that it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the Health Privacy Principles
- **Lawful authorisation** – the transfer is permitted or required by an Act (including an Act of the Commonwealth) or any other law (see Section 11.3).

13.3 Linkage of health records (HPP 15)

HPP 15 does not affect the ability of NSW Health services to link personal health information electronically with other NSW Health entities. All other HPPs must be complied with prior to any linkage. Such linkage should occur in line with the general terms of this Manual and relevant NSW Health policies.

HPP 15 will apply to the linkage of health records at a state or national level between the public and private sectors, or between two or more private health services. It requires that such a system must be "opt-in", i.e. that a patient must give "express consent" to participate in such a system. Any such consent must comply with the requirements outlined in Section 5.4 and must be documented.

There are two exemptions to HPP 15. These are:

- a health service is not obliged to comply with the provision if "lawfully authorised or required not to comply", or non-compliance is otherwise permitted or reasonably contemplated under a law or
- where the linkage is for research purposes and has been approved in accordance with the Statutory guidelines on research.

14 Complaints handling

Health services should always try to resolve information privacy complaints quickly and informally, using formal processes as a last resort. However, privacy law provides patients with a right to make a formal complaint.

A formal complaint would generally include:

- a complaint submitted on an internal review application form, and/or
- correspondence which refers to the privacy internal review process, and/ or
- correspondence which indicates that the applicant is aggrieved or dissatisfied with the treatment of their health (and/or personal) information and the health service is unable to arrive at resolution through informal processes.

In circumstances where the HCCC has requested that a health service respond to a complaint which involves both clinical and privacy issues, the health service should address the privacy issues as comprehensively as possible in response to the HCCC complaint. In addition, the health service should advise the HCCC that the aggrieved patient is also entitled to seek a privacy internal review from the relevant health service regarding the privacy aspects of the complaint. The privacy internal review application form and information sheet should be enclosed with the response to the HCCC together with the appropriate contact details for the health service.

The *Health Records and Information Privacy Act 2002* requires health services to use the complaints process set out in Part 5 of the *Privacy and Personal Information Protection Act 1998*.

Guidelines for management of complaints using these processes are set out in NSW Health Internal Review Guidelines. If you receive a complaint under privacy legislation, you should refer to this document.

14.1 General principles

Individuals can make a complaint about a health service's management of personal health information privacy on the grounds that the health service has contravened a Health Privacy Principle, a Health Privacy Code of Practice or Regulation. Such complaints should be referred immediately to the agency's Privacy Contact Officer (see Section 6.2).

All privacy complaints, enquiries about privacy, and requests for internal review, should be treated as serious matters. A complaint must be in writing, addressed to the health service concerned and made within six months of the individual becoming aware of the alleged contravention (unless the health service agrees to a longer timeframe).

A person is not required to identify the particular HPP that he or she considers has been breached. Health services are obliged to review any such complaint received and to identify the specific HPPs which arise.

Privacy law provides first for a health service to conduct an internal review of a complaint. The internal review provisions allow individuals to seek a review of certain conduct of an agency, in circumstances where the individual believes that the agency has breached the terms of the privacy laws. Internal reviews are to be undertaken in accordance with the NSW Health Internal Review Guidelines which reflect the provisions of the *PPIP Act* and are based on guidelines issued by Privacy Commission NSW.

Where a person raises general concerns as to how personal or personal health information is being handled and does not indicate that they are personally aggrieved by the conduct, agencies should seek to address the person's concerns by reference to the agency's existing information management policies and guidelines for complaints handling. For example, a patient may express concern about the number of staff accessing their health record. The patient may not seek a privacy internal review of this practice, rather some explanation and reassurance regarding staff duties of confidentiality.

Where the person's concerns cannot be resolved through existing policies and guidelines, an agency must provide the person with information relating to their rights to an internal review under privacy laws, and the requirements for lodging an application for review. If the person chooses to exercise these rights, the terms of the Internal Review Guidelines will apply.

In some cases, the privacy complaint may relate to, or be linked with other complaints lodged with the health service. When this occurs, the privacy officer should alert the decision maker and vice versa, so that the two investigation processes can be managed concurrently.

14.1.1 NSW Civil & Administrative Tribunal (NCAT)

If the complainant is not satisfied with the outcome of the application, the complainant may then appeal the issue to the NSW Civil & Administrative Tribunal (NCAT).

Where a person lodges an action before the NCAT, the health service should notify the NSW Ministry of Health Legal and Regulatory Services Branch of the application, and a notification should also be made to the Treasury Managed Fund (TMF).

Further guidance

- GL2006_007: NSW Health Internal Review Guidelines

14.2 Sanctions

If the Tribunal finds the complaint against the health service proven, it may order the health service:

- to pay damages of up to $40,000 to the applicant by way of compensation for any loss or damage suffered because of the conduct
- to refrain from any conduct or action in contravention of a HPP
- to comply with a HPP
- to correct information which has been disclosed and/ or
- to take specified steps to remedy any loss or damage suffered by the applicant.

There are also criminal offences relating to **public sector officials** found guilty of intentionally disclosing or using personal health information. Penalties include:

- the individual to pay a fine of up to $11,000 or to be imprisoned for up to 2 years, or both
- to confiscate any money or other benefit alleged to have been obtained by the individual in connection with the offence.

14.3 Notifying individuals of a breach of their privacy

From time to time, a health service may become aware that an individual's privacy has been breached. This may have occurred deliberately, for example, by a staff member inappropriately accessing health records, or inadvertently, for example, when the wrong 'Mrs Jones' is contacted by a health service, personal information is uploaded to the internet in error, or clinical hand-over notes are found in a public place.

There is no obligation within the *Health Records and Information Privacy Act 2002* or any law, to notify the individual when their privacy has been breached. However, as a matter of good practice, consideration should be given as to whether the affected individual(s) should be notified.

When notifying individuals of a breach of their privacy, the health service should provide them with the opportunity to apply for privacy internal review in accordance with the NSW Health Internal Review Guidelines.

In general, if sensitive personal information has been made publicly available (e.g. via the internet), or if there is a risk of serious harm as a result of a privacy breach, the affected individuals should be notified. Risk of harm can include psychological, physical, financial or other. The health service should also notify the Ministry of Health which may notify the Information and Privacy Commission NSW.

Further guidance

- The Office of the Australian Information Commissioner has published the 'Data Breach Notification – A guide to handling personal information security breaches – April 2012', available at: www.oaic.gov.au/publications/

Whilst NSW Health is not obliged to comply with this document, it is a useful guide to assist health services in this area.

14.4 Breach of Health Privacy Principle(s) by an employee

Where it is found, or suspected, that a staff member has breached one or more of the Health Privacy Principles (HPPs), the health service should investigate the allegations in accordance with the requirements for privacy internal review in order to determine:

- Whether a breach has occurred
- The nature and extent of the breach
- Whether the breach occurred inadvertently or deliberately
- What course of action to take with regards to the staff member
- Whether to notify the affected individual(s) (if they were not the complainant), see Section 14.3.

When the finding constitutes a breach of privacy, action taken by the health service should be commensurate with the nature, scale and seriousness of the breach. Action can range from remedial (discussion, counselling, training) to disciplinary (warning, termination). However, any action should always comply with NSW Health policy and be managed in accordance with policy obligations.

Further guidance

- PD2005_225: Disciplinary Process in NSW Health – Framework for Managing the Disciplinary Process
- PD2006_007: Complaint or Concern about a Clinician
- GL2006_007: NSW Health Internal Review Guidelines

15 Common privacy issues

Sometimes staff may seek further information about broader interaction with other government agencies, specific projects or matters that cut across the HPPs outlined in Sections 7-13. In recognition of this, Section 15 of the Manual is designed to provide a Quick Reference Guide on common privacy issues in NSW Health.

15.1 Third party health care providers

The HPPs recognise that health care providers should be able to access personal health information necessary for ongoing care and treatment purposes.

Outside these circumstances however, access must be sanctioned by one of the exceptions listed in Health Privacy Principle 11 (see Section 11 Using & disclosing personal health information (HPPs 10 & 11)).

The following guidelines are provided to assist health services to ensure privacy issues are addressed when disclosing personal health information to third party health care providers.

15.1.1 Informing patients

Patients should be made generally aware that:

- access to a patient's health record will be available to the patient's treating health care providers and others who will be involved in their care within the health system
- it is normal practice to provide the patient's GP and other providers involved in ongoing care with a discharge referral.

The NSW Health Privacy Leaflet for Patients includes this information.

Further guidance

- Section 7 Collecting personal health information (HPPs 1-4)
- Appendix 5 Pro forma Privacy Leaflet for Patients

15.1.2 Health practitioner obligations

Recognition that health care providers involved in ongoing care may access patient information is designed to enhance treatment provision by ensuring service providers have ready access to information relevant to care. In these circumstances however, health care providers also have both a legal and professional obligation to ensure they exercise this right appropriately.

15.1.3 Addressing patient concerns

Sometimes, patients may have greater concerns about how and when some sort of information is made available. This is particularly likely to be the case in relation to personal health information collected for services such as sexual health, genetics, sexual assault, child protection. Health services should be aware of these concerns and endeavour to address them.

Further guidance

- Section 15.9 Information-specific laws and policies

15.1.4 Conclusion of care

When an episode of care concludes for whatever reason (including the death of a patient), the right of access by a health practitioner to the health record is normally terminated at the same time.

Access may still be authorised for purposes other than patient care, such as clinical audit or research, provided these fall within the HPPs.

15.1.5 Discharge referrals to GPs and others

It is standard practice to provide a patient's GP and other external health care providers involved in ongoing care, (for example, community health services, early childhood health services) with a discharge summary.

Admission processes are relied upon to check the accuracy of a patient's GP details on each admission. In circumstances where an error is found within a discharge summary, the revised summary should be re-issued to the correct GP.

Where GPs or other providers request access to the patient's personal health information more than 3 months after their discharge or conclusion of care, extra care must be taken to ensure that access is being sought for ongoing care purposes. Either the request must be made in writing stating the purpose for access and this request stored as part of the patient's health record, or the circumstances of the request must be fully documented on the patient's health record.

Further guidance

- Section 9.2.4.5 Transmission of electronic documents (discharge referrals/ summaries)

15.1.6 Records of a patient's family members

Requests by health care providers for access to the health records of members of a patient's family cannot be treated as exceptions to the rule and must be accompanied by the written consent of the person to whom the health record relates (or an authorised representative).

Further guidance

- Section 5.6 Authorised representative
- Section 11.2.3.4 Genetic information
- Section 11.2.9 Disclosure on compassionate grounds
- Section 12 Patient access and amendment (HPPs 6, 7 & 8)

15.2 Requests from state and federal police

15.2.1 Where disclosure to police is authorised by patient

All access requests to the health record should be referred to the Health Information Service.

Where a patient has authorised the police to have access to information from his/her health records, this may be supplied following provision of a written request by the police and consent by the patient. The health information should be assessed and the disclosure limited to fit the terms of the request and consent. Clinical staff should liaise with the Health Information Service, or facility equivalent, prior to release of information to police.

15.2.2 Where access is not authorised by patient

Section 11.2.7 provides detailed guidance on where the *HRIP Act* allows law enforcement agencies, including the police to access personal health information. These should be followed where the patient has not consented or has refused to release their information.

15.2.3 Search warrants

Compliance with a search warrant is required by law and record keepers are advised that they should inform their immediate supervisor of any official demand for access to information.

Further guidance

- Section 11.2.7 Law enforcement agencies, including police
- Section 11.3.6 Search warrants and subpoenas

15.2.4 Police interviews

15.2.4.1 Interviews with patients

Except in the case of declarations from dying patients, permission to interview a patient should only be given where the patient agrees and where the treating health practitioner is of the opinion that the patient's medical condition permits the conduct of an interview.

Consideration should also be given to other factors such as the needs of other patients who may be in the same room, infection control issues and staff hand over times. The police visit should be documented in the health record.

15.2.4.2 Interviews with patients under the age of 16

If a patient is under the age of 16, a parent or legal guardian should be present during police questioning. Alternatively, a parent or legal guardian can give permission for another person to be there.

If the patient is 16 or over, they can nominate an independent adult to be present during police questioning.

15.2.4.3 Interviews with victims of sexual assault

Where police wish to interview the victim of a sexual assault, the relevant local Sexual Assault Service should be contacted.

15.2.4.4 Interviews with staff

Where police wish to interview staff in relation to a matter that is unrelated to their work (for example, they may have witnessed a car accident or a crime), the health service will have no involvement in any interview, as it is purely a matter between the staff member and police.

Where police seek to conduct an interview about an incident related to the health service (for example, in relation to a coronial matter or an assault on hospital premises) the staff member should be advised to inform their supervisor and representative organisation, or a support person should be offered.

Further guidance

- Section 11.2.3 To prevent a serious and imminent threat to health or welfare
- Section 11.2.7 Law enforcement agencies, including police
- Section 11.3.4 Reporting "serious criminal offences"

15.3 Child protection records

15.3.1 Restrictions on access to Child Protection Counselling Records

NSW Health has special policies for Child Protection Counselling Service (CPCS) records. In accordance with these policies, the following applies:

- Child Protection Counselling Service records are generally maintained separately from the general health record
- Child protection health records can be linked to the general health record only via a notation that a "*confidential health record exists*"

- Access to the content of the record for care and treatment purposes is restricted. Access must be sought via a designated contact in the Child Protection Counselling Service, who in turn will seek patient consent.

15.3.2 Child Sexual Assault Services

Records relating to child sexual assault are generally held by Sexual Assault Services, and will also be subject to the above requirements. Counselling records relating to sexual assault may also be subject to sexual assault communications privilege.

Further guidance

- Section 11.3.2 Child protection
- Section 11.3.6 Search warrants and subpoenas
- PD2013_007: Child Wellbeing and Child Protection Policies and Procedures for NSW Health
- PD2010_065: Subpoenas
- Child Wellbeing and Child Protection – NSW Interagency Guidelines
  www.community.nsw.gov.au/kts/guidelines/info_exchange/introduction.htm

15.4 Health examinations of school children

Parental permission for health examinations of school children is usually recorded by the parent's signature on the school health card following a statement of consent to the examination.

The results of vision and hearing tests and other health findings cannot be communicated to teachers or recorded on the Education Department Pupil Record Card unless additional consent is obtained or this was provided for in the original consent advice.

15.5 Use of interpreters

Patients whose preferred language is a language other than English should be informed in their own language of their rights to access their health records.

Professional interpreters should be made available. This is particularly important where the information to be discussed is complex, likely to be considered sensitive by the patient or where the patient may be at risk of harm, for example, if they are victim to domestic violence or sexual assault. The gender of the interpreter should also be taken into consideration.

Health staff may need to request the services of an interpreter if they have difficulty understanding a patient or are unsure about whether the patient has understood information given to them.

When collecting information or seeking consent for the use of data, a professional interpreter should be used to ascertain the wishes of the patient and obtain informed consent if appropriate.

When adapting the pro forma Privacy Leaflet for Patients (see Section 7.4.5) for more specialised services, consideration should also be given to appropriate translations of the revised leaflet into languages other than English.

Interpreters are obliged to keep confidential any personal information they may access in the course of their duties.

Further guidance

- PD2006_053: Interpreters – Standard Procedures for Working with Health Care Interpreters
- PD2006_084: Domestic Violence – Identifying & Responding

15.6 Legal claims and insurance

15.6.1 Claims manager and Treasury Managed Fund

Cooperation is to be afforded where the health service has sought cover from the NSW Treasury Managed Fund (TMF) in response to an actual or anticipated legal claim. Access to personal health information which is relevant to the claim may be provided to the solicitor acting on behalf of a Local Health District or Specialty Network, in cases covered under the Treasury Managed Fund Statement of Cover.

Such access does not require authorisation from the patient. The LHD Risk Manager and Hospital Executive Managers should be informed of such requests.

Further guidance

- Section 12.5.4 Access by staff responding to a complaint, claim or investigation

15.6.2 Patient's legal representative

Where the patient's legal representative has been authorised to view the complete health record of a patient, the health care facility should make such access available within facility premises.

If requested, the facility should attempt to provide photocopies. Such photocopying is to be at the expense of the legal representative and charged at current rates, as set out in the relevant Information Bulletin.

Further guidance

- PD2006_050: Health Records & Medical/ Clinical Reports – Charging Policy
- IB2013_032: Health Records & Medical/ Clinical Reports – Rates

15.6.3 Patient's insurer

Where the request is made for information related to an insurance or compensation claim, a 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. Patient consent is required for disclosure of additional health records.

Further guidance

- Section 11.2.1 Directly related purpose
- Section 11.2.2.1 Where a third party seeks access
- Section 12.5.4 Access by staff responding to a complaint, claim or investigation

15.7 Enquiries about hospital patients, including media

15.7.1 Enquiries about patients

A health service may neither confirm nor deny the current or past presence of a person, unless the enquirer already knows that the patient is present.

Where staff are satisfied the enquirer knows the patient is present they may indicate ward details provided they believe that to do so would not be contrary to the interests of the patient. If in doubt, or where there is evidence the patient may be at risk, the patient should be consulted prior to details being provided to a third party.

If the enquirer is requesting information about the patient, the staff member should make reasonable attempts to contact the patient and transfer the telephone call to the patient, or to request that the patient returns the call.

Where a patient requests that no information be released, or that information be released only in certain circumstances, such as in an immediate post-operative period, this request should be complied with and any patient lists used by the enquiry section may be modified accordingly.

15.7.2 Other safeguards for enquiries sections

Health services should ensure that patient lists used by enquiries sections do not include diagnosis and are kept out of view of the public. Where possible, wards should be identified by name, letter or number rather than by specialty (e.g. Ward A instead of psychiatric ward, colorectal unit etc.).

15.7.3 Media queries

No personal health information about a patient should be released to a media agency without the consent of that patient. If the patient is conscious and can communicate, he/she should be asked whether information may be disclosed. If the patient is deceased, is unconscious or is otherwise lacking capacity, the "authorised representative" (see Section 5.6) must be asked before information is disclosed.

Any decision to disclose material held on a deceased patient should also have due regard to any view expressed by the patient to staff prior to death, either in writing, or as recorded in the patient's health record.

15.7.3.1 Responsibility for media liaison

All media enquiries should be directed to the health service's Media Unit. A designated Media Liaison or Public Affairs Officer should always be the first point of contact for the media. A Media Officer from the Ministry of Health is available via the on-call 24 hour media pager. Health services also have an on-call Media Liaison Officer.

15.7.3.2 Accident victims

Information released about accident victims should be limited to broad, de-identified information, such as the number of casualties, sex, approximate age and whether injuries are critical, serious or minor.

15.7.3.3 Information about health practitioners

Information provided to a media agency regarding a patient should not refer to a health practitioner in private practice.

If information is released to a media agency, an assurance should be sought from the facility concerned that only information about health practitioners working for the health service may be released.

15.7.3.4 Recordings of patients, including photography, sound and video recordings for media purposes

Recordings of a patient, including photography, sound and video recordings, should not occur outside clinical care requirements unless the patient requests this or agrees in writing.

The patient should be informed about the purpose of the photography, sound or video recordings, e.g. therapy, health promotion, publicity etc.

Further guidance

- Section 9.2.2 Images and photography

15.8 Fundraising

Personal health information should not be used or disclosed for the purpose of fundraising or gaining public support unless there was a specific consent from the patient at the time of collection of that information, for example, as part of the admissions process, or unless the patient has subsequently been provided with information about the fundraising and they have signed and returned a consent form. The right to withhold consent should be made clear at the time such consent is sought also that their health care will not be affected in the event they choose not to participate.

Patients have a right to withdraw consent and to have their names and addresses removed from any lists held. To this end:

- direct mail should contain a statement of the addressee's right to have his/her name removed from mailing lists
- correspondence should clearly display the name and full address of the sender
- they should be advised that any action taken prior to the withdrawal of consent may still occur.

Committees involved in fundraising and/or public support campaigns should ensure that names and addresses are deleted from mailing lists promptly when requested.

Further guidance

- Section 5.4 Consent

15.8.1 Limits on what information may be used

The information which may be released with consent is limited to name and address. Information relating in any way to a patient's health status is not to be included in information made accessible for fundraising and public support campaigns.

15.8.2 Use of mailing lists

A mailing list should not be used for any purpose other than that for which it was compiled unless further consent is obtained from each person on that list. Mailing lists should be accurate, complete and up to date. When no longer current, lists should be properly disposed of (see Section 9.1 Retention and disposal of personal health information).

A mailing list should be securely stored and should remain at all times in the custody of the health service which originally compiled the list. A member of a fund raising committee may not have access to mailing lists held by that committee once they have ceased to be a member of the committee.

Committees are not to release to or exchange identifiable information with any third party.

15.8.3 Organisations with a commercial interest

Information regarding patients must not be provided to organisations which may have a commercial interest in such information, even though it may be sought ostensibly for the purpose of offering assistance or advice.

15.9 Information-specific laws and policies

All personal health information is generally considered to be sensitive personal information, dealing as it does with matters that are extremely personal and which a patient will generally expect to be shielded from public disclosure. The terms of the *HRIP Act* are based on adopting and reflecting these expectations.

As noted in Section 11.2.1, sometimes patients will have different expectations about how some of their personal health information will be used or disclosed. These expectations can be based on their own cultural or personal background, family situation, a feeling that certain information is particularly stigmatising, or additional legal restrictions imposed on use or disclosure. Some common examples include services provided to patients by specialist genetics services, drug and alcohol services or sexual health services and the special restrictions which apply by law to the release of adoption and organ donation information.

NSW Health has issued a number of statewide policies to guide staff on management of personal health information in some of these circumstances. These are summarised below, with information on the relevant laws and policies included. Staff are advised to access these policies for more detailed guidance on the particular areas.

15.9.1 Aboriginal health information

The NSW Ministry of Health and the *Aboriginal Health and Medical Research Council* (AHMRC), the peak body representing Aboriginal Community Controlled Medical Services in NSW, have developed the *NSW Aboriginal Health Information Guidelines* (AHIG). These guidelines provide a framework of ethical and culturally sensitive protocols for the collection and use of personal health information relating to Aboriginal and Torres Strait Islander peoples in New South Wales.

Requests for access to Aboriginal health information and the collection of information (including personal health information) from Aboriginal communities must demonstrate compliance with the terms of the AHIG, and information users must agree in writing to adhere to its terms. It is recommended that such requests should be referred to the Centre for Aboriginal Health for consideration and advice.

Further guidance

- NSW Aboriginal Health Information Guidelines (AHIG)
  www.ahmrc.org.au
  Contact: Centre for Aboriginal Health, NSW Ministry of Health

15.9.2 Adoption information

Any application by a person involved in an adoption for access to adoption-related information (including birth-related information) should be referred to the Adoption Information Unit of Family & Community Services (FACS).

Information from the health record may be released on receipt of an authorised request from FACS.

Care should be taken to withhold the identity of the biological parents (or information that may assist in identification), unless it is evident that this information is already know to the applicant.

Where a request is received from a person or organisation other than FACS, the facility should contact FACS to establish the bona fides of the inquirer before releasing the information.

To prevent matching of adopted persons or adoptive parents with biological parents in health records, copies of correspondence should be kept physically separate from the biological parents' health records.

Further guidance

- PD2010_050: Adoption Act 2000 – Release of Information

15.9.3 Service-based policies

15.9.3.1 Genetics services

Information collected by a NSW Genetics Service often includes an extensive family tree with information about the health status of other relatives without their knowledge or permission. Specialised genetics records should be stored securely and preferably separately. Genetic health records should be held indefinitely due to the potential value of family health tree information to other family members, particularly in following generations.

15.9.3.2 Third party access – insurers and employers

The results of predictive or pre-symptomatic testing generally relate to healthy people but may indicate risk of developing a disorder in later life. If access to predictive test results is requested by third parties, such as insurers and employers, patient consent must be sought prior to disclosure. There is no obligation on a health practitioner to disclose information to such a third party.

15.9.3.3 Third party access – genetic relatives

Where a health practitioner anticipates a situation where information will be obtained from a patient which may be of interest or potential benefit to other family members, he or she should discuss this with the patient

prior to treatment being commenced or as part of protocols for ordering tests. Through counselling, individuals should be encouraged to accept their own responsibilities with regard to the information needs and rights of others.

Since 2014, the HRIP Act has included provisions and processes for genetic information, which allows for the disclosure of genetic information to genetic relatives without patient consent, albeit in very limited circumstances, in accordance with guidelines issued by the NSW Information and Privacy Commission.

Further guidance

- Section 11.2.3.4 Genetic information
- NSW Health Ethical Code Governing the Provision of Genetics Services (1998)
- NHMRC Guidelines for Genetic Registers and Associated Genetic Material (1999)

15.9.3.2 Sexual assault services

Health services have local policies for the management of information collected by NSW Sexual Assault Services.

In accordance with these policies:

- Health records are generally maintained separately.
- Health records can be linked to the general health record only via a notation that a 'confidential health record exists'.
- Access to the content of the health record for care and treatment purposes is restricted. Access must be sought via a designated contact in the Sexual Assault Service, who in turn will seek patient consent.

Health records subject to the Sexual Assault Communications Privilege should be marked confidential and transported in sealed envelopes.

15.9.4 Service-based practices

Policies for dealing with the collection of personal health information by stand-alone drug and alcohol or sexual health services, are generally developed at the operational level. Staff should contact the local service for further details on how health records are managed both in hard copy and as electronic health records.

Patients attending these types of stand-alone services will often have expectations about how their information has been used. As a result, these Services tended, as a matter of practice, to develop specific practices in the management of the personal health information they collect.

Further guidance

- Section 16 Electronic health information management systems.

15.9.4.1 Sexual health services

Some sexual health services are provided as stand-alone services, not integrated into a general hospital, and therefore patients may have the expectation that these records are held separately to any general health records relating to them, and that these records would not be shared with staff outside the health service without their consent. Most sexual health services have policies which rely on extensive patient consents to determine how and when information about the services received by a patient can be disclosed.

Where sexual health service records are part of the LHD's electronic health record (eHR) system, auditing which targets access to these records is an appropriate system support for protecting privacy of sensitive information.

Staff should refer to local policies with regards to the management of electronic health records.

In addition, the *HRIP Act* allows for disclosure for emergency purposes (see Section 11.2.3), and with lawful authorisation (see Section 11.3). Other exemptions listed in Section 11 also continue to apply.

Special statutory restrictions are also imposed on access to information about a person's HIV status under the *Public Health Act 2010*.

Further guidance

- Section 4.1.3 Public Health Act 2010
- Section 11.2.3.3 Public Health Act 2010 – Notification of public health risk
- Section 15.9.6 Managing public health risks
- Section 16 Electronic health information management systems

15.9.5 Organ and tissue donor information

In order to protect the privacy of grieving relatives of a recently deceased donor, it is not permissible to disclose any information which could enable the identification of the donor of a transplanted organ or tissue.

Issues relating to the disclosure of information in such cases are comprehensively dealt with under section 37 of the *Human Tissue Act 1983*. Under this provision the identity of the donor and recipient of transplanted tissue (whether living or deceased) must not be disclosed except in the following circumstances:

- with the consent of the person to whom the information relates, or in the case of a deceased person, the authorised representative for the deceased person (see Section 5.6)
- in connection with the administration or execution of the *Human Tissue Act*
- in connection with research which has Human Research Ethics Committee (HREC) approval
- for the purposes of any legal proceedings or reporting of such proceedings
- with other lawful excuse.

Further guidance

- PD2005_341: Use and Retention of Human Tissue including Organ Donation, Post Mortem Examination and Coronial Matters

15.9.6 Managing public health risks

The *Public Health Act 2010* establishes a range of provisions which impact on the management of personal health information. These provisions ensure the Secretary, NSW Health, has appropriate powers to take action when a matter involving risk to public health arises (such as outbreaks of food poisoning or disease).

15.9.6.1 Reporting of certain medical conditions and diseases

The *Public Health Act 2010* also establishes requirements for doctors, hospital Chief Executive Officers and laboratories to notify certain diseases to Public Health Units.

Further guidance

- IB2012_011: Notification of Infectious Diseases under the *NSW Public Health Act*
- PD2012_047: Notifiable Conditions Data Security and Confidentiality
- NSW Health Infectious disease control guidelines available at: www.health.nsw.gov.au/infectious/pages/default.aspx
- PD2009_023: Management of People with HIV Infection Who Risk Infecting Others
- PD2005_068: Tuberculosis Management of People Knowingly Placing Others at Risk of Infection
- PD2005_162: Health Care Workers Infected
- *Public Health Act 2010*
- *Public Health Regulation 2012*

15.9.6.2 Contact tracing

NSW Health has guidelines in place providing for contact tracing. Contact tracing involves informing a person that he or she may have been at risk of infection because he or she was in contact with a person with a

communicable disease. The guidelines are based on a number of factors, including consideration of the risk of exposure and the nature of the disease.

For those conditions followed up by public health units, contact tracing is undertaken confidentially and all efforts are made to protect the identity of the person with the communicable disease. This person is referred to as the 'index case'.

Under clause 39B of the Public Health Regulation 2012, the Secretary, NSW Health (or delegate) may notify a person who is believed to have been in contact with a person suffering from a specified medical condition of measures to be taken (e.g. diagnosis, treatment and prevention) to prevent further transmission of infection.

The identity of a contact may be obvious to the person being notified, however, the terms of the regulation still enable contact tracing to proceed. Whilst in such cases the health service involved would not be in breach of the patient privacy, the health service should make every effort to protect the identity of the index case where ever this is possible within the scope of contact tracing.

In situations where authorisation has been given for contact tracing without the consent of the index case, it is appropriate for the index case to be informed of this and given a final opportunity to provide consent.

Further guidance

- PD2005_184*:* Contact tracing guidelines for the sexually transmissible diseases and blood borne viruses
- PD2009_023: HIV – Management of people with HIV infection who risk infecting others
- *Contact:* Local Sexual Health Service or Public Health Unit.

15.9.6.3 Undertaking public health inquiries

Section 106 of the *Public Health Act 2010* gives the Secretary, NSW Health (or delegate) broad powers to inquire into any matter relating to the health of the public. A person authorised by the Secretary (or delegate) for the purposes of such an inquiry is entitled to enter premises inspect and copy health records. These powers can only be exercised however where the person has been issued with a Certificate of Authority by the Secretary, NSW Health (or delegate) under section 106 of the Act.

15.10 Deceased patients

Privacy law continues to apply to the information of a deceased person for 30 years after their death.

When dealing with the information of deceased persons, a health service should have regard to:

- special provisions allowing disclosure of information for compassionate purposes (see Section 11.2.9)
- provisions allowing the authorised representative (normally the executor of the deceased person's will) to make a decision on behalf of a person (see Section 5.6)
- other grounds allowing use or disclosure provided for under HPPs 10 and 11
- provisions relating to access to information held by a health service provided for under the *Government Information (Public Access) Act*.

Any decision to disclose material held on a deceased patient should also have due regard to any view expressed by the patient prior to death, either in writing, or as recorded in the patient's health record. This would include any advanced directive, such as an Advanced Care Directive, made by the patient.

15.11 Telehealth

The primary objective of telehealth is to enhance access to and equity of health services for residents of both metropolitan and rural areas of New South Wales by enabling real time, remote clinical consultation and more efficient transmission, storage and sharing of patient information. The medico-legal and privacy issues for

telehealth consultations for both image transfer and clinical consultations follow the same rules as for face-to-face consultations, and therefore the principles contained in this Manual can be applied to telehealth consultations.

In addition, at the start of telehealth consultations, verbal consent must be provided and documented in the patient's health record. This provides an accurate record of the treatment plan the patient is receiving via telehealth as part of their overall care. Having this information correctly captured allows effective communication between clinicians regarding care, treatment and medication details which may assist in the event of future presentations to other NSW health services.

Video or sound recordings of telehealth consultations generally do not occur, in the same way that such recordings are generally not made for face-to-face consultations. Recordings which capture personal health information are subject to strict storage and retention rules as set out in the *State Records Act 1998* and the *Health Records and Information Privacy Act 2002* (see Section 9 Retention, security and protection (HPP 5)).

Further guidance

- *Contact:* the Telehealth Implementation Unit, NSW Agency for Clinical Innovation (ACI) on telephone (02) 9464 4666.

15.12 Community health records

15.12.1 Group houses/hostels

Comprehensive health records of patients residing in Ward-in-a-house, group houses or hostels should continue to be maintained and securely stored.

The non-institutional nature of group houses and hostels may pose particular difficulties to managing the privacy of personal health information and special precautions should be taken to ensure that patient privacy is maintained.

Health records should be stored in a secure place, inaccessible to patients and visitors. Health records maintained and kept at the home/hostel should be limited to:

- registration book: content may vary but should include identification data and referrals accepted and refused
- day book
- card index or mini-file: should include identification data, referral information and medication details.

15.12.2 Group sessions

Individual patient intake forms (or equivalent) should be placed behind a chart divider to separate them from the group form and protect the privacy of each patient.

15.12.3 Family consultations

In the case of family consultations, information on other family members may be recorded in the health record of the family member who is the patient. Extreme care should be taken to safeguard the privacy of other family members.

Information about family members, or other third parties, which the patient (or person seeking access to the health record) may be unaware of, must not be disclosed without consent from that individual.

Where multiple family members are patients of the health service, family records must be maintained as individual records.

Where release of information on an individual has been appropriately authorised, care should be taken to ensure that only information relating to the specific episode indicated by the individual patient is released.

Further guidance

- Section 11.2.3.4 Genetic information
- Section 15.9.3.1 Genetics services
- PD2007_094: Client Registration Policy

15.13 Maintaining the health record

This section is designed to provide guidance on key obligations in managing the health record. It is the responsibility of the record keeper to ensure compliance with those provisions of the *HRIP Act* and this Manual which apply to health records. Also refer to Section 9, and Section 16 of this Manual.

Clearly visible privacy notices should be attached to health records or flagged in electronic systems. See **Appendix 4.3** for a sample privacy notice.

15.13.1 Quality of health records

The health record should comply with Section 9 and be sufficiently detailed and comprehensive to:

- provide effective communication to health care providers
- provide for a patient's effective, ongoing care
- enable evaluation of the patient's progress and health outcome
- retain its integrity over time.

As the primary purpose of keeping health records is to enable better patient care, it is important that the information in health records is current, clear, accurate, complete and readily available.

A number of documentation models exist and practices may vary according to local needs. Whatever model or method is used, the health record should be clear and comprehensible to others.

15.13.2 Accuracy and completeness

To ensure that the health record is accurate and complete:

- information should be recorded at the time of consultation or procedure or as soon as it becomes available
- entries should generally be made by those collecting the information or present when the information was collected
- each entry should be signed by the clinician, their designation, the date and time clearly legible electronic signatures must be managed with care to ensure equivalent accuracy is maintained
- alterations or deletions should not be made original incorrect entries should not be erased but lined through so the original entry remains readable, and such action should be explained and signed
- the senior treating health practitioner should periodically review the health record for correctness
- there should be an audit trail for electronic health records.

Further guidance

- Section 10 Accuracy
- Section 16.3.4 Auditing
- PD2012_069: Health Care Records – Documentation and Management
- NSW Health Patient Matters Manual, Section 9
  www.health.nsw.gov.au/policies/manuals/Pages/patient-matters-manual.aspx

15.13.3 Control of health records

Control over the movement of health records is of the utmost importance. An adequate health record tracking system, tailored to local needs, is essential to facilitate prompt record location and ensure that patient care does not suffer and that privacy is not breached.

Systems for transporting health records within a health service should be well supervised to ensure that health records are not accessible by unauthorised persons.

No health record should be removed from its home location without the following details being recorded in an appropriate system:

- health record number
- patient name
- destination/location of the health record
- person responsible for/in possession of the health record
- date health record was removed.

Records subject to the Sexual Assault Communications Privilege should be marked confidential and transported in sealed envelopes.

15.13.4 Removal

Health records should be kept under adequate security as outlined in Section 9 and the original only removed from the control of the health service upon receipt of a court subpoena, statutory authority, search warrant, coronial summons (see Chapter 9 of the Patient Matters Manual) or by order of the Secretary, NSW Health.

Whenever the original health record leaves a health service, a copy of that record should, where possible, be made beforehand and kept.

15.13.5 Transfer

If it is necessary to transfer a paper-based health record outside the health service it should be transferred under seal, marked 'confidential' and where possible sent by courier.

Where health records are transported by staff members, for example as part of a Community Health Service, care must be taken to ensure records are not in public view, and should be securely transported in a closed non-transparent container.

It is the responsibility of the staff member who receives the health record to ensure it is kept in a secure location to prevent loss and unauthorised access.

Electronic transfer of health records must also be secure.

Further guidance

- Section 9.2.4 Safeguards when delivering and transmitting information

15.13.6 Storage, archiving and disposal

Disposal of health records should comply with Section 9.1 and the *State Records Act*, and take into account the type of information contained in a health record and possible future demand for it as well as the needs of individual health services. In particular the following should be considered:

- use of health records for patient care, medico-legal purposes and research and teaching
- archival value
- provisions of the *Evidence Act 1995* and the Statute of Limitations
- available storage space
- requirements under the provisions of the *State Records Act 1998*.

Similar standards for maintaining privacy and security should be maintained for health records in archival or secondary storage as for health records in current use.

Further guidance

- PD2012_069: Health Care Records – Documentation and Management
- Patient Matters Manual Section 9
- General Disposal Authority (GDA 17) Public health services: Patient/Client Records (State Records NSW) www.records.nsw.gov.au

15.13.7 Health facility closures

When a facility is closed and ceases to operate, each responsible unit should create a register that includes details of:

- Health records destroyed
- Health records retained
- Health records transferred to other locations
- Location(s) where the health records have been transferred to
- Officers who undertook closures
- The full name of the facility being closed and the facility receiving the records should be clear on the register, along with the date of closure, the date range of records destroyed and the date range of records transferred and the range of medical record numbers if possible.

Details of records that are to be destroyed should include as a minimum:

- the location where the health records were created
- the patient's surname and given name
- the patient's sex
- the patient's date of birth
- the last date of contact with the facility
- the general nature of the health records
- the date for destruction or the date destroyed.

15.13.8 Transfer of General Practice health records to public health services

NSW State Records provide a General Disposal Authority (GDA No 42) Public Health Services: general practice health records.

The authority applies to general practice health records in the custody and control of public health services and the transfer of these records to the patient (or their representative) on request or their destruction after suitable retention periods have been met.

Further guidance:

- General Disposal Authority (GDA No 42) Public Health Services: general practice medical records Available at: www.records.nsw.gov.au

15.14 NSW data collections

15.14.1 NSW Health data

Statistical information and other data are submitted to the Ministry of Health for inclusion in a number of centrally maintained data collections. Collection of such data is required or authorised by a range of health legislation, such as the *Public Health Act 2010*, the *Health Administration Act 1982*, and the *Private Health Facilities Act 2007*, the *Home and Community Care Act 1985* (Commonwealth).

15.14.2 Health Information Resources Directory (HIRD)

Central data collections and the data elements they contain are documented in the Health Information Resources Directory (HIRD). The HIRD is the authoritative central registry for data collections and metadata. It is the responsibility of each data custodian, or other delegate of the data sponsor, to ensure that the data collection for which he or she is responsible, if in scope, is recorded in HIRD.

Health services that also own or administer data collections should also keep a register of those collections. Such a register should include (as a minimum):

- Data collection name
- Collection sponsor
- Collection custodian and contact details
- Statement of the collection's purpose
- Any Act or Regulation authorising the collection
- Statement of whether the collection includes personal health information.

15.14.3 Staff roles

All staff employed within the health system have a duty to maintain, within their roles, the privacy, integrity and security of data held and managed by their work unit.

Data sponsor : Each data collection has a nominated data sponsor who undertakes the duties of ownership on behalf of the relevant health service, including:

- Defining the purpose of the data collection
- Establishing the scope and coverage of the collection
- Defining access and custody arrangements

Data custodian: The data sponsor appoints a custodian for each data collection who is responsible for:

- Data storage and disposal
- Compliance of data with relevant legislation and policies
- Administration
- Quality assurance
- Data access and release

15.14.4 Access to data collections

Where data collections contain identifying or potentially identifying information, HPP 10 and 11 will apply to any requests for use and access. While access may be authorised under any of the exceptions listed in HPP 11(1) and 11(2), the most common are likely to be where:

- the access relates to the primary purpose for which the data was collected (for more detail, see Section 11.1)
- the access is for a directly related purpose, which would be "reasonably expected" by the individual (see Section 11.2.1)
- the access is required or authorised by law (see Section 11.3)
- use or disclosure is required for management or research purposes (see Section 11.2.4).

Where access is sought for management or research purposes, the NSW Privacy Commissioner's Statutory guidelines on research and the Statutory guidelines on management apply. These guidelines provide for requests for such access to be approved by a Human Research Ethics Committee (HREC). In relation to data collections held by the NSW Ministry of Health, applications should be made to the NSW Population and Health Services Research Ethics Committee (NSW PHSREC).

Based on the evaluation report of the HREC or the PHSREC, the appropriate data custodian will approve or reject the request and advise applicants in writing of the committee's recommendation, including reasons for denial of access and any conditions or restraints applying.

15.14.4.1 Conditions of access

If access is granted the principal applicant must sign an agreement to apply, as a minimum, the standards of privacy protection contained in the *HRIP Act*, and to abide by any other conditions or constraints (relating to charges, monitoring requirements etc.) on the use of the data set by the data custodian.

Although NSW Health will endeavour to facilitate access to data by bona fide applicants, access is not guaranteed. Each request will be judged, and access granted or denied, on its own merits. The information supplied will always be the minimum required to meet a project's objectives.

Access, when granted, will be subject to the terms and conditions set out in an agreement, to be drawn up by the data custodian and signed by the principal applicant. If access is refused, the reasons for refusal will be documented in a written response from the data custodian. The applicant may choose to amend the proposal in the light of this response and re-submit it, in which case the assessment process will need to be repeated.

15.14.4.2 Record linkage

Linkage of specific data is authorised under the *HRIP Act* provided the linkage is necessary for the purposes of management or research and the Statutory guidelines have been complied with.

Linkage of whole health records for the purposes of establishing an ongoing health record must, however, comply with HPP 15.

15.14.4.3 NSW Population and Health Services Research Ethics Committee

The NSW Population and Health Services Research Ethics Committee (NSW PHSREC) is constituted as a Human Research Ethics Committee (HREC) in accordance with NHMRC guidelines for the protection of privacy in the conduct of medical research. The committee undertakes assessment of requests for access to personal information held in data collections maintained at central administration. The PHSREC also considers:

- proposals for data use or issues requiring ethical advice referred by NSW Ministry of Health officers
- multi-centre research proposals
- proposals referred by HRECs
- proposals for data and health record linkage.

16 Electronic health information management systems

The continued expansion and growth in global technologies is aiding the development of many new electronic health information management systems to improve efficiencies and quality of care within NSW Health.

Electronic health information management systems require robust security and governance policy and practices in place to maintain the integrity of the data and the trust of the people of NSW.

Such policies assist staff compliance with their privacy obligations and reduce the risk of privacy and security breaches through effective communication and management processes (see Section 14.4 Breach of Health Privacy Principle(s) by an employee).

The fundamental principles for management of, and access to, electronic health information management systems are provided below (see Section 16.3 Fundamental principles). These principles should be incorporated into local security and governance practices in order to maximise the benefits of electronic health information management systems, and minimise the privacy and security risks.

16.1 Electronic health records

Electronic health records differ from paper health records in ways that warrant special consideration. Firstly, it is possible to have a single electronic health record simultaneously accessible at multiple sites, giving more people access. Secondly, it is possible to control access to an electronic health record in ways that are not possible with a paper health record.

Health records may consist of both hard copy (paper) and electronic health records (sometimes referred to as a *hybrid* record). When handling personal health information, it is important to consider whether relevant health information is held in the other format and whether both the electronic health record and the hard copy health record need review when making a decision about the health information contained in the records.

16.2 Data collections and data warehousing

Data collections and data warehousing systems are subject to the *Health Records and Information Privacy Act 2002*, and therefore Health Privacy Principles 10 and 11 regarding use and disclosure of personal health information will apply (see Section 11 Using & disclosing personal health information (HPPs 10 & 11)). There are a range of reasons why NSW Health will establish data collections, including:

- Provision of clinical care to patients and in some circumstances their families
- Public health surveillance
- Performance monitoring
- Service management and improvement
- Service planning and policy development
- Allocation of funds
- Public accountability
- Research in accordance with guidelines by the NHMRC (see Section 11.2.4 Management, training or research)

Health Privacy Principles 10 and 11 allow for the above uses of personal health information as they fall into the definition of a 'directly related purpose' (see Section 11.2.1 Directly related purpose), or meet the criteria for a management or research activity (see Section 11.2.4 Management, training or research).

NSW Health data collections can often be based on statistical or other data and so may not include 'identifiable' information. Where identifiable information is not included, privacy laws do not apply (see Section 16.2.1 Identified and de-identified data).

16.2.1 Identified and de-identified data

Within some NSW Health data collections, data may be classified in various ways such as: fully identified data, semi-identified data, re-identifiable data and de-identified data.

Whilst these may be valid and useful classifications for management of information, they are not used in the privacy laws. When considering the implications under privacy law for the access, use or disclosure of health information held in any context within NSW Health, regard needs to be had to the definitions of "personal health information" used in the HRIP Act. These provide that "information about an individual whose identity is apparent or can reasonably be ascertained from the information" is personal information and therefore regulated by the HRIP Act.

If there is a reasonable chance that the information is potentially identifiable, it will fall within the ambit of the privacy law controls. Clearly, whether information can be considered de-identified will be dependent on the specific circumstances which arise in any disclosure.

Privacy laws and policies only apply to identified data (also see Sections 5.1 Health information, and 5.2 Personal information).

16.3 Fundamental principles

Electronic systems facilitate access to personal health information. Staff and health providers should be aware of their obligation to restrict access to what is clinically necessary for patient care, or otherwise authorised under the law. Systems to audit user access and protect security to ensure compliance with these obligations should be in place.

The following principles provide guidance on how to address privacy issues when accessing electronic health information management systems, such as electronic health records (eHRs), NSW Health data collections, and data warehousing systems.

16.3.1 Privacy and confidentiality undertakings for staff

Staff must sign a privacy undertaking on employment and when gaining access to electronic health information management systems (see Appendix 3) outlining their responsibility to observe the Health Privacy Principles and duties of confidentiality. Where staff are provided access to a number of health information management systems, each system should be clearly identified in the privacy declaration.

16.3.2 Training and informing staff

Staff accessing electronic health information management systems must be informed and regularly reminded of their responsibilities to patient privacy and confidentiality. This can be achieved through a combination of staff induction, staff meetings, training, staff newsletters, notices, posters, and so on.

Providing staff with brief privacy messages at critical decision points in the system may also be an effective way of reminding staff of privacy obligations.

Some examples of electronic notifications for NSW Health staff are:

> Example: "Remember you must only access the information necessary to fulfil your work duties. If in doubt, check with your senior manager, or for further information go to: www.health.nsw.gov.au/patients/privacy/Pages/default.aspx"

Example: "You are bound by strict privacy law and NSW Health privacy policies regarding access to, use and disclosure of the personal health information contained in <ABC> system. The principal governance policy governing <ABC> system is: <XYZ>
The principal privacy policy is: NSW Health Privacy Manual for Health Information.
The principal privacy law is: NSW Health Records and Information Privacy Act 2002

Example: "If you suspect a breach of the privacy or security of the <ABC> system, you should discuss this with your manager, and consider contacting the Privacy Contact Officer for your organisation. Details are available at: www.health.nsw.gov.au/patients/privacy/Pages/privacy-contacts.aspx"

Further guidance

- Section 6.1.2 Staff training
- Section 14 Complaints handling

16.3.3 Access protocols

The approval process for access applications to electronic health information management systems should have robust governance systems to minimise opportunities for inappropriate disclosure. Features of robust access protocols include:

- Access to electronic health information management systems should be provided on a 'needs only' basis. Consideration should be given as to whether access to de-identified data, or limited identified data, is sufficient for the staff member's work requirements.
  Where access to identifiable data is required, the purpose/ business requirement should be documented as part of the access application.
  Access should be specific to job requirements or for the duration of a project, and then reviewed/ renewed at appropriate intervals, depending on the business needs.
- Staff who are provided with access to any system containing personal health information should have a secure individual login which should not be shared. Health organisations should have processes in place to discourage the sharing of passwords. Sharing passwords significantly decreases security controls and exposes the health information to unauthorised access, use and disclosure. Generic passwords should only be used for systems which contain de-identified information, generally used for analysis and reporting.
- Robust processes must be in place for regular review of access arrangements for individuals, for example, where staff move into a new role access levels should be reviewed and if staff leave the organisation their log-ins to all systems, including remote access functionality, should be disabled.
- Clear criteria for approval for access to an electronic health information management system must be followed and documented, for example:
  - Confirmation of each applicant's employment status and position
  - The name of each system to which access is to be provided and the associated level of access to be provided
  - Confirmation that the application has been approved by the Line Manager
  - Confirmation that each applicant/manager has provided requirements for access
  - Confirmation that if access is for a specific project, the requested time period for access is appropriate to business needs and liaison with system administrators will occur to ensure access is reviewed as approved.

16.3.4 Auditing

Audit functionality is a mechanism which can be incorporated into electronic health information management systems holding personal health information.

Data quality which includes the completeness and accuracy of health information (both demographic and clinical) is an important principle in the management of health information. As part of audit functionality, electronic health information systems should have control mechanisms that assess and report on data quality.

Audit records of access to health records should be maintained on an ongoing basis. Audit reports and notifications should be generated regarding access to health records as required. Systems should be in place to appropriately manage security and minimise unauthorised breaches of access.

Key elements that support a robust audit process may include:

- Name and ID of employee or contractor
- Position or designation of employee or contractor
- Name and MRN of health record accessed
- Date and time access commenced
- Date and time access ceased
- Section(s) of the health records viewed
- Where possible, Device ID (eg. MAC ID and IP Address)

Audit functionality may include:

1. Creation of an audit record each time a user accesses, creates, updates or archives personal health information via the system.

2. A log which uniquely identifies the user, the data subject (the patient), the function performed by the user, and the time and date at which the function was performed.

3. When a record is updated, a record of the original data, who entered the new data, and at which time and date, should be retained.

4 A log of message transmissions used to transmit messages containing personal health information.

The organisation should carefully assess and determine the retention period for these audit logs, with particular reference to clinical professional standard and legal obligations, in order to enable investigations to be carried out when necessary.

16.3.5 Informing patients

Patients should be made generally aware that their personal health information will be managed using electronic systems, and that systems are in place to prevent unauthorised access to information held in these systems. This is included in the pro forma Privacy Leaflet for Patients (see Appendix 5).

Further guidance

- Section 9.2.3 Computer systems and applications
- Section 11 Using & disclosing personal health information (HPPs 10 & 11)

16.4 *Evidence Act 1995*

The *Evidence Act 1995* does not preclude electronic records being used as evidence unless their veracity can be questioned. To minimise the possibility of records converted from paper being open to challenge, the equipment and scanning processes must be capable of scanning to 100% accuracy with no possibility of corruption or manipulation of images. Control processes should be implemented to ensure that images cannot be altered between scanning and storage or while stored. Scanning processes should include quality control checking mechanisms to ensure the captured image is legible and reproducible.

16.5 Accountability

Information accountability means that the use of information should be transparent so it is possible to determine whether a particular use is appropriate and in accordance with the 15 Health Privacy Principles, and that the system enables individuals and health services to be held accountable for any misuse of information.

Accountabilities should be clearly articulated for the system which delivers the record to ensure the integrity of electronic health records. Backup and recovery solutions are required in case of disaster.

Whoever enters the information into the health record is accountable for the accuracy of the information. Some staff will have additional responsibility for ensuring the overall accuracy of the health record and the care with which the details have been documented.

16.6 Access and quality control

The area over which the electronic health record is available is important, i.e. individual facility, campus or health service. The broader the system, the greater the need for tighter network and access controls.

Where the electronic health record system covers multiple facilities, the health records may contain a mix of entries from different sources or partial copies of health records from other facilities. The ability to maintain a single, logical health record in this situation is critical. This can be achieved through various means such as individual patient identifiers, employee numbers, appropriate labeling of each transaction and adequate version control. Identification and authentication of the person making the entry is important.

Electronic health records should meet the same records documentation quality standards and requirements as paper records, for example, when inaccuracies are identified in the health record, the inaccurate data should not be deleted. The original data must be retained as a contemporaneous record, flagged that it has been identified as inaccurate and the amendment entered as a dated notation, making the record complete and accurate.

16.7 Patient access

It is important to ensure that the right of patients to access their own health records is not compromised by the introduction of electronic health records. Health facilities should have local policies, compliant with privacy obligations which allow patients access to their health records. Electronic health records should be retained in compliance with the State Records General Disposal Authority (GDA) 17 Public Health Patient Records. Fees and charges raised for access to health information should be consistent with NSW Health policy. Adequate viewing, printing and copying facilities should be readily available. All requests for access to health information must be in accordance with Health Privacy Principles 6 & 7 (see Section 12 Patient access and amendment (HPPs 6, 7 & 8)).

16.8 National eHealth Record

The National eHealth Record, also known as the Personally Controlled Electronic Health Record (or PCEHR), is being trialled by the Commonwealth Government Department of Health, as an optional way for patients to view a summary of their health records online.

Participating NSW Health agencies will make health information available to the health providers which individuals have authorised as part of the eHealth Record program.

It is not intended that the eHealth Record will replace, or should be relied upon in place of, health records maintained by a health service. The purpose of the eHealth Record is to provide individuals with an online tool to manage and view a summary of their health records in accordance with Commonwealth eHealth policy.

For further information, go to: www.ehealth.gov.au

Further guidance

- Section 9.2.3 Computer systems and applications
- Section 11 Using & disclosing personal health information (HPPs 10 & 11)
- Section 13.3 Linkage of health records (HPP 15)
- PD2013_033: Electronic Information Security Policy – NSW Health
- PD2012_069: Health Care Records – Documentation and Management

Appendix 1 - List of relevant policies

A.1.1 NSW Health policies, guidelines and information bulletins

Note: the titles and reference numbers are subject to change. Refer to the NSW Health website publications page for current information. Go to: www.health.nsw.gov.au/policies/Pages/default.aspx

A
Aboriginal and Torres Strait Islander Origin – Recording of Information of Patients and Clients (PD2012_042)
Adoption Act 2000 – Release of Information (PD2010_050)
C
Cancer Registry – Notifying Cancer Cases to the NSW Central Cancer Registry (PD2009_012)
Chaplaincy Services and Privacy Law (IB2008_044)
Child Wellbeing and Child Protection Policies and Procedures for NSW Health (PD2013_007)
Client Registration Policy (PD2007_094)
Client Registration Guideline (GL2007_024)
Code of Conduct (PD2012_018)
Communications – Use & Management of Misuse of NSW Health Communications Systems (PD2009_076)
Complaint Management Policy (PD2006_073)
Complaint or Concern about a Clinician – Principles for Action (PD2006_007)
Consent to Medical Treatment – Patient Information (PD2005_406)
Contact Tracing Guidelines for Sexually Transmissible Diseases and Blood Borne Viruses (PD2005_184)
Coroners' Cases and the *Coroners Act 2009* (PD2010_054)
Corporate Governance & Accountability Compendium for NSW Health
D
Data collections – Process for Approval of New or Modified (PD2005_155)
Data collections – Disclosure of unit record data for research or management of health services (PD2012_051)
Disciplinary Process in NSW Health – A Framework for Managing (PD2005_225)
Domestic Violence – Identifying and Responding (PD2006_084)
E
Electronic Information Security Policy – NSW Health (PD2013_033)
F
Framework for Managing the Disciplinary Process (PD2005_225)
G
Goods & Services Procurement Policy (PD2014_005)
H
Health Records and Medical/ Clinical Reports – Charging Policy (PD2006_050)
Health Records and Medical/ Clinical Reports – Rates (IB2014_054)
Health Care Records – Documentation and Management (PD2012_069)
Health Care Workers Infected (PD2005_162)
HIV – Management of people with HIV infection who risk infecting others (PD2009_023)
Home and Community Care Minimum Data Set Version 2 – Collection & Reporting Requirements (PD2008_050)
Human Tissue – Use and Retention including Organ Donation, Post Mortem Examination and Coronial Matters (PD2005_341)

I
Information & Privacy Commission Guideline: Use & disclosure of genetic information without consent (IB2014_065)
Inpatient Statistics Collection (ISC) (PD2005_210)
Interpreters – Standard procedures for working with health care interpreters (PD2006_053)
M
Mandatory Training Requirements in Policy Directives (PD2014_023)
Management of People with HIV Infection Who Risk Infecting Others (PD2009_023)
Mental Health Information and the Health Records and Information Privacy Act 2002 (IB2010_044)
N
Notifiable Conditions Data Security and Confidentiality (PD2012_047)
Notification of Infectious Diseases under the *NSW Public Health Act 2010* (IB2013_010)
NSW Health Internal Review Guidelines (GL2006_007)
NSW Health & Civil Chaplaincies Advisory Committee NSW Memorandum of Understanding (PD2011_004)
P
Privacy Management Plan NSW Health (PD2005_554)
Protecting People and Property: NSW Health Policy and Standards for Security Risk Management (IB2013_024)
S
Subpoenas (PD2010_065)
T
Tuberculosis Management of People Knowingly Placing Others at Risk of Infection (PD2005_068)
W
Work Health and Safety – Better Practice Procedure (PD2013_050)
Z
Zero Tolerance: Response to violence in NSW Health workplace (PD2005_315)

A.1.2 Other government policies

Available via relevant government websites

NSW State Records

- General Disposal Authority (GDA No.17) Public health services: Patient/Client Records
- General Disposal Authority (GDA No. 36) Imaged or microfilmed records
- General Disposal Authority (GDA No. 42) Public Health Services: general practice records
- Record Keeping In Brief 48: Disposal at a Glance
- Record Keeping In Brief 51: Destroying Digital Records – When pressing delete is not enough
- Destruction of Records (Guideline 3)

NSW Department of Premier & Cabinet

- NSW State Digital Information Security Policy
- NSW Government Social Media Policy & Guidelines Family & Community Services (FACS)
- Child Wellbeing and Child Protection – NSW Interagency Guidelines

A.1.3 Policies which govern the private sector

National Health & Medical Research Council:

- Use and disclosure of genetic information to a patient's genetic relatives under section 95AA of the Privacy Act 1988 (Commonwealth) – Guidelines for health practitioners in the private sector.

Office of the Australian Information Commissioner:

- Data breach notification - A guide to handling personal information security breaches (April 2012).
- Australian Medical Association: Clinical images and the use of personal mobile devices, available at: https://ama.com.au/article/clinical-images-and-use-personal-mobile-devices

Appendix 2 – List of relevant laws

Note:

Legislation relevant to the operation of NSW Health can be viewed via the Legal Compendium at:
www.health.nsw.gov.au/legislation/Pages/Legal-Compendium.aspx
NSW legislation can be viewed at: www.legislation.nsw.gov.au/
Commonwealth legislation can be viewed at: www.comlaw.gov.au

Acts referred to in Privacy Manual	Privacy Manual Reference
Births, Deaths and Marriages Registration Act 1995	Section 11.3.13
Children and Young Persons (Care and Protection) Act 1998	Section 11.3.2, Section 15.3
Community Services (Complaints, Reviews and Monitoring) Act 1993	Section 11.3.10
Coroners Act 2009	Section 11.3.5
Crimes Act 1900	Section 11.3.4
Evidence Act 1995	Section 11.2.2, Section 12.5, Section 15.13.6, Section 16.2
Government Information (Public Access) Act 2009	Section 4.2, Section 12.2, Section 15.10
Guardianship Act 1987	Section 5.6
Health Administration Act 1982	Section 4.1, Section 11.3.13, Section 15.14.1
Health Care Complaints Act 1993	Section 11.3.2
Health Records and Information Privacy Act 2002	Throughout the Manual
Health Services Act 1997	Section 7.1, Section 11.3.1, Section 11.3.13
Home and Community Care Act 1985 (Commonwealth)	Section 11.3.13
Human Tissue Act 1983	Section 15.9.4
Migration Act 1958 (Commonwealth)	Section 11.3.12.3
Mental Health Act 2007	Section 4.1.2, Section 11.3.9
Ombudsman's Act 1974	Section 11.3.8,
Poisons and Therapeutic Goods Act 1966	Section 11.3.1
Privacy and Personal Information Protection Act 1998	Section 2, Section 4.1, Section 6.5, Section 14
Privacy Act 1988 (Commonwealth)	Section 4.1.4, Section 13.2.1
Private Health Facilities Act 2007	Section 11.3.1, Section 11.3.13, Section 15.14.1
Public Health Act 2010	Section 4.1.1, Section 4.1.3, Section 8.2, Section 11.2.3.3, Section 11.3.13, Section 15.9.3, Section 15.9.5, Section 15.14.1
Social Security (Administration) Act 1999 (Commonwealth)	Section 11.3.12.1
State Records Act 1998	Section 4.2, Section 9.1, Section 15.13.6
Surveillance Devices Act 2007	Section 9.2.2.3
Veterans' Entitlement Act 1986 (Commonwealth)	Section 8.2, Section 11.3.12.2
Work Health and Safety Act 2011	Section 11.3.11

Appendix 3 – Pro forma Privacy undertaking

This proforma is an example only, and if necessary, may be adapted to local needs in consultation with the Privacy Contact Officer for your health service (see Section 6.2 for details).

(**Reference:** Section 6.4, Section 9 and Section 16.1 of the NSW Health Privacy Manual for Health Information)

Privacy undertaking

I, ...(name), understand that while I am employed by the

..... (name of health service) I will have access to personal health information collected from patients/ clients that is protected by privacy law. I undertake not to knowingly access any personal information, (such as information contained in a patient's health record, including in an electronic health record/ XXXX data collection(s)/ XXXX data warehouse) unless such information is essential for me to properly and efficiently perform my duties.

I recognise and accept that my access to, holding and use of this information is subject to the Health Privacy Principles contained in the *NSW Health Records and Information Privacy Act 2002* (copy of Health Privacy Principles attached). In order to fulfil this undertaking, I will not divulge any personal information regarding individual persons, except as allowed by the Health Privacy Principles.

I undertake to comply with other information privacy and security procedures as stipulated by NSW Health policies* in relation to any personal information that I access in the course of my duties. In order to fulfil this undertaking I will ensure that, so far as is within my control, such information, whether in the form of paper documents, computerised data or in any other form, cannot be viewed by unauthorised persons, and that the information is stored in a secure and orderly manner that prevents unauthorised access.

I further undertake to inform (my supervisor/ title of relevant officer) immediately if I become aware of any breach of privacy or security relating to the information that I, or other staff, access in the course of my duties.

Signed	Witnessed
.....	.....
(name)	(name)
.....	.....
(signature)	(signature)
.....	.....
(position)	(position)
.....	.....
Date	Date

*** Relevant NSW Health policy directives include:**

- NSW Health Privacy Manual for Health Information
- Data Collections – Process for Approval of New or Modified
- Electronic Information Security Policy – NSW Health
- NSW State Digital Information Security Policy

A.3.1 Contractual provisions

The types of provisions which should be included where data is transferred to an external contractor for work include:

Acknowledgement of privacy laws

- **Recognise** that the information must be handled in accordance with relevant privacy laws.

Purpose

- Clearly **define the purpose** for which it will be used and the disclosures (if any) allowable under the contract
- Require the contractor **not to use or disclose** the information for any other purpose without appropriate written consent of the health service
- **Require the data to be destroyed** or returned to the health service after use or at the termination or completion of the Contract

Security

- Information provided must be handled in a **secure manner**
- The **contractor is responsible** for ensuring the appropriate security for and disposal of the information
- **No copies** to be made of the information unless the copies are reasonably necessary for the defined purpose or made with the written permission of the health service
- Contractor must ensure that all information sent to it under the Contract via disc, ftp, email, gopher, Internet or other media is **moved to a secure computer storage** as soon as received
- The contractor to **ensure information is disclosed to as few persons** within its organisation as are reasonably necessary for the defined purposes for which the information was supplied

Appendix 4 – Pro Forma Privacy notices

These pro forma notices are examples only, and if necessary, may be adapted to local needs in consultation with the Privacy Contact Officer for your health service with the Privacy Contact Officer for your health service (see Section 6.2 for details).

A4.1 Fax cover sheet

(**Reference:** Section 9.2.3.2.)

Privacy notice:

The information contained in this fax message is intended for the named addressee only. If you are not the intended recipient you must not copy, distribute, take any action reliant on, or disclose any details of the information in this fax to any other person or organisation. If you have received this fax in error please notify us immediately.

A4.2 General privacy notice (eg. for use in emails and other electronic transmissions)

(**Reference:** Section 9.2.4.5.)

Privacy notice:

If you are not the intended recipient you must not use, disclose, copy or distribute this communication. If you believe you have received this message in error please ensure you delete it and notify the sender.

A4.3 Health records

(**Reference:** Section 15.13)

Privacy notice:

This is a confidential health record.

Do not access, read or remove this health record from this facility unless authorisation is given.

A4.4 Patient charts/ End of patient bed

(**Reference:** Section 9.2.1)

CONFIDENTIAL INFORMATION

This is a confidential health record.

Do not access, read or remove this health record unless you are authorised.

Patients, relatives and visitors must speak to a staff member if they wish to view any part of the patient health record.

Appendix 5 – Pro Forma Privacy Leaflet for Patients

(**Reference:** Section 7.4)
The pro forma Privacy Leaflet for Patients is to be used by health services for distribution to patients. The leaflet content may be updated from time to time. For the latest version, and for details on how to obtain copies, contact the Privacy Contact Officer for your health service. Contact details are available via the NSW Health privacy webpage at: www.health.nsw.gov.au/patients/privacy/Pages/default.aspx

Pro forma Privacy Leaflet for Patients

Our obligations

We are committed to treating your personal information in accordance with privacy law.

This leaflet explains how and why we collect personal information about you, how you can access your information and how your information may be used within the NSW public health service or disclosed to other parties.

Collection of your personal information

We collect information directly from you wherever possible. If this is not possible, or in an emergency, we may also need to collect information from a family member, friend, carer or other person who can help us to provide you with appropriate health care.

Security of information collected

Your information may be held in a variety of ways within the NSW public health service. Most commonly, your information may be held as a paper health record, and/ or an electronic health record forming part of a secure computerised database. Some information may also be held in the form of an image including x-ray or photograph, or as an audio or video recording.

We follow strict rules and policies regarding the secure storage of personal information in all formats in order to protect your information from unauthorised access, loss or other misuse.

Use or disclosure of information

Your personal health information held either in paper or electronic format may be used by the NSW public health service, or disclosed outside the health service, to enable appropriate care and treatment to be provided to you. For example, your information may be used or disclosed as follows:

- to other treating health services, hospitals or medical specialists involved in your care and treatment
- to your nominated GP, including information provided with your discharge referral documents
- to contact you at home regarding follow-up appointments
- to your carer to assist them with your care
- to the Ambulance Service of NSW
- to process pathology tests, x-rays, and so on
- to contact you for feedback on the services you have received from us to help us evaluate and improve our services
- for billing and debt recovery
- to pastoral care workers, including hospital chaplains, providing spiritual and pastoral care
- to students and other staff for training purposes
- to other health services and authorised third parties to help prevent a serious and imminent threat to someone's life, health or welfare, such as in an emergency

- to claims managers and associated persons for the purpose of managing a complaint, legal action, or claim brought against the health service or a treating health professional
- for purposes relating to the operation of the NSW health service and treatment of our patients, including funding, planning, safety and quality improvement activities

If you do not wish for us to collect, use or disclose certain information about you, you will need to tell us and we will discuss with you any consequences this may have for your health care.

The law also allows or requires for your personal health information to be disclosed to other third parties, for example:

- to State and Commonwealth government agencies for statutory reporting purposes, such as to report notifiable diseases, for example, cancer and infectious diseases, to report births and deaths, and to provide Medicare details.
- to researchers for public interest research projects as approved by a Human Research Ethics Committee
- to other health services or law enforcement agencies, such as the police, if you provide us with information relating to a serious crime, including assault, domestic violence, child abuse, and so on
- to other agencies where the information relates to the safety, welfare or wellbeing of a child or young person
- to comply with a subpoena or search warrant if your personal information is required as evidence in court

Personally Controlled Electronic Health Record (PCEHR)

Participation in the National e-Health Record, the PCEHR, is optional. If you wish to participate, you will have to provide your express written consent. NSW Health will not share your health information with the PCEHR program without your consent. For further information, go to: www.ehealth.gov.au

Access to your information

You are entitled to request access to all personal information including your health record held by health services in NSW. Normally you will be asked to apply for access in writing and provide identification. You may be charged a fee if you request copies of your personal information or health record. Requests for access to information will be responded to as soon as possible, or in most cases no later than 28 days.

Access to your personal information may be declined in special circumstances, such as where giving access would put you or another person at risk of mental or physical harm.

If you believe the information we hold about you is incorrect or an error has been made, please let us know and we will correct it or add a notation to your health record.

Requests for access to your health record should be addressed either to the Health Information Service or to the manager of the health service facility you attended.

Contact us

If you have questions or a complaint about the privacy of your personal information, please contact:

The Privacy Contact Officer

[Name of Health Service, address and telephone number]

Appendix 6 – Privacy Information Leaflet for Staff

For copies of this leaflet please contact the Privacy Contact Officer for your health service (see Section 6.2 for details).

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 requirement 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.

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

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, Section 5.3

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 Internal Review Guidelines

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 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 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 assist, 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.
- 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, incidents, patient safety, the health service.

- To manage a legal action or claim brought by the patient against the health service.

Ref. Privacy Manual, Section 11

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, Sections 5.4 and 11.2.2

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, Section 7 and Appendix 5

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. Health records and computer screens should not be accessible to unauthorised people.
Ref. Privacy Manual, Section 9

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, and a fee 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 check 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.

In addition, to correct clinical information, patient information such as name, address, contact person and current GP name must be correct for each encounter.
Ref. Privacy Manual, Sections 10 (Accuracy) and 12 (Access and Amendment)

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.
- Health facilities have an audit capacity in their electronic health records (eHRs) and other systems to investigate staff access to health records. **Staff must only access health records where this is required for direct patient care delivery or is required in the course of their employment.**
- Database managers and custodians must ensure compliance with all privacy principles. Health 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. Ref: NSW Health Privacy Manual for Health Information, Section 15.9.
- 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. Ref: NSW Health Privacy Manual for Health Information, Section 11.2.7.

Further information available at:

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

Appendix 7 – Consent Guide for Medico-Legal Requests

Acknowledgment:

This guide has been adapted from a check list provided by the Northern NSW Local Health District (2013).

Type of request	Notes
The section references refer to sections contained within the NSW Health Privacy Manual for Health Information.	
Coroner	Reference: Section 11.3.5
Continuing patient care	Reference: Section 11.2.1
Child Death Review Team – NSW	Reference: Section 11.3.10
Deceased patient	Reference: Section 5.6
Deceased patient – Compassionate grounds	Reference: Section 11.2.9
Defence Force Recruitment	Non-health related purpose, therefore consent is required.
Family and Community Services (FACS) Chapter 16A of *Children and Young Persons (Care and Protection) Act 1998*	All Chapter 16A requests must be processed through the Central Contact Person for the facility or health service. All responses must be written using the 16A template. References: NSW Health policies on Child Protection and Wellbeing – Information Exchange, and Privacy Manual for Health Information, Section 15.3
****Health Care Complaints Commission**	Reference: Section 11.2.8, Section 11.3.7
Insurance	Scanned or photocopies of consent normally acceptable. Reference: Section 11.2.2
Notice of Claim (NOC)	An NOC must be accompanied by a valid consent. In most cases, the medico-legal officer processing the NOC will need to contact the respondent's insurer or legal representative, and advise that a valid consent must be forwarded from the patient that they are seeking information about. Do not confirm or deny whether the person has attended hospital, until the consent has been submitted.
Out of Home Care – Family and Community Services (FACS)	Need to make sure consent is from the 'authorised representative', in this case, FACS must provide a copy of the Court Order stating their 'parental rights'. Reference: Section 5.6 – authorised representative
Out of Home Care – Other person/body/ agency (Not FACS)	Need to make sure consent is from the 'authorised representative', in this case, where FACS have granted another body or agency parental rights, a copy of the court order must be produced in conjunction with a valid consent to release information signed by the nominated FACS Officer. Reference: Section 5.6 – authorised representative.
Patient/Personal	Reference: Section 12.
Police (expert certificates, medical statements)	Reference: Section 11.2.7 The need for consent depends on the circumstances. The need to assist law enforcement agencies with their investigative work must be balanced with the need to protect patient privacy. Section 11.2.7 provides guidance on how to achieve this balance.
Police (serious crime and fraud, blood alcohol test results, missing persons, public risk, forensic evidence, foreign bodies)	Such requests should be discussed with your Manager. Reference: Section 11.2. and Section 11.3.4.

Type of request	Notes
The section references refer to sections contained within the NSW Health Privacy Manual for Health Information.	
Registrar of Births, Deaths and Marriages	Consent is not required when validating or seeking missing birth/death information only. Reference: Birth registration, forms and related legislation (PD2005_509).
Research/Clinical Trials	The need for consent will depend on the terms of the research ethics approval. Reference: Section 11.2.4.
Solicitor	The need for consent will depend on the circumstances, for example, whether the solicitor is acting on behalf of a staff member, or on behalf of the patient. Reference: Section 15.6.
Subpoena (including police)	Reference: Section 11.3.6.
Worker's Compensation	Non-health related purpose, therefore consent is required.
Worker's Compensation – billing purposes	Purpose is 'directly related'. Reference: Section 11.2.1.1

*** Consent: For a consent for release of information to be valid, it must:**

- be in writing, either on letterhead, or if via email, it must include a detailed signature block. The consent may be a photocopy or scanned version of the original document. If there are reasonable grounds to doubt the authenticity of the document, an original copy of the consent may be sought. (see Section 11.2.2)
- clearly state the name of the individual authorising the release
- clearly state to whom they are authorising the release
- be dated within a suitable timeframe of the original request being submitted, either within 3 months for a specific or 'one off' disclosure, or within 12 months (see *Section 5.4.1*).

**** Investigative agencies:**

Health Care Complaints Commission is an 'investigative agency'. The rules for disclosure to an investigative agency within NSW and within all jurisdictions within Australia are the same (*see Section 11.3.7*).

It is more important to establish whether the purpose for disclosure is authorised. Requests from Commonwealth agencies, organisations or bodies are generally authorised (*see Sections 11.2.6 and 11.2.8*).

Index

*References in **bold** denote the principal reference.

NOTES

NOTES

SHPN (LRS) 150001