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.

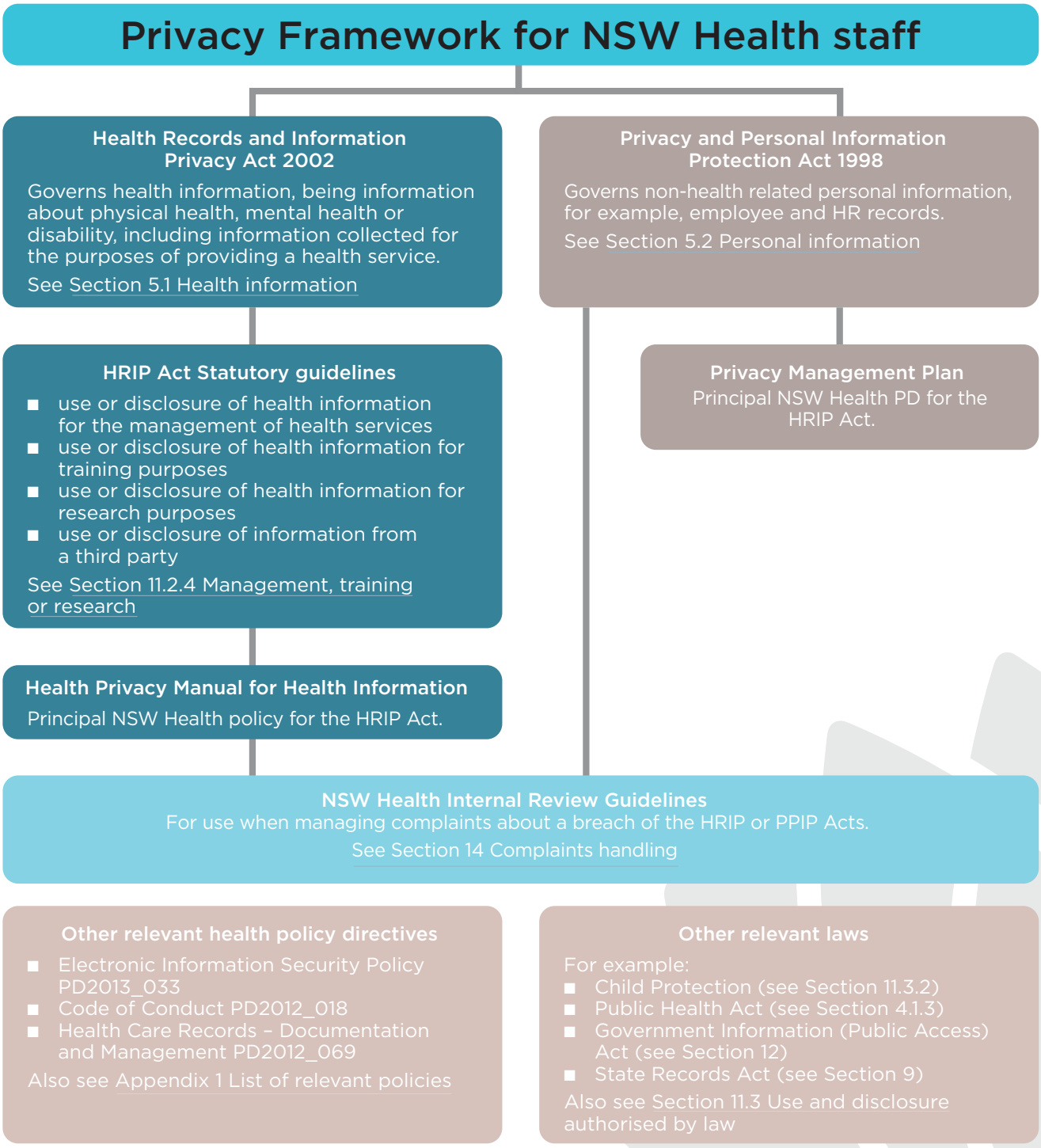
3.7 What other NSW Health resources should be considered

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.