Policy Directive

Ministry of Health, NSW
73 Miller Street North Sydney NSW 2060
Locked Mail Bag 961 North Sydney NSW 2059
Telephone (02) 9391 9000 Fax (02) 9391 9101
http://www.health.nsw.gov.au/policies/

Privacy Management Plan

Document Number PD2015_036

Publication date 14-Sep-2015

Functional Sub group Corporate Administration - Governance
Corporate Administration - Records
Clinical/ Patient Services - Pharmaceutical
Personnel/Workforce - Conduct and ethics

Summary This Policy Directive contains information about management of personal information held by NSW Health. Information about management of health information is contained in the Privacy Manual for Health Information.

Replaces Doc. No. Privacy Management Plan - NSW Health [PD2005_554]

Author Branch Legal and Regulatory Services

Branch contact Legal and Regulatory Services 02 9391 9092

Applies to Local Health Districts, Board Governed Statutory Health Corporations, Chief Executive Governed Statutory Health Corporations, Affiliated Health Organisations, Public Health System Support Division, Community Health Centres, Dental Schools and Clinics, NSW Ambulance Service, Ministry of Health, Public Health Units, Public Hospitals, NSW Health Pathology, Cancer Institute (NSW)

Audience All staff

Distributed to Public Health System, NSW Ambulance Service, Ministry of Health

Review date 14-Sep-2020

Policy Manual Not applicable

File No. 15/3399

Status Active

Director-General

This Policy Directive may be varied, withdrawn or replaced at any time. Compliance with this directive is **mandatory** for NSW Health and is a condition of subsidy for public health organisations.

POLICY STATEMENT

PRIVACY MANAGEMENT PLAN

PURPOSE

This Privacy Management Plan explains how NSW Health complies with obligations under the *Privacy and Personal Information Act 1998* (PPIP Act).

Information about how NSW Health complies with obligations under the *Health Records and Information Privacy Act 2002* (HRIP Act) is contained in Privacy Manual for Health Information.

This plan sets out our commitment to respecting the privacy rights of NSW Health employees and members of the public. It is produced in accordance with the requirement for a Privacy Management Plan under section 33 of the PPIPA and demonstrates how NSW Health ensures compliance with PPIPA, the procedure for applying for an internal review and other matters related to privacy and personal information, and the protection of personal information held by NSW Health.

The 2015 plan updates references and structural changes which have occurred since the initial plan was put in place in 2005.

MANDATORY REQUIREMENTS

All staff of NSW Health are required to comply with the PPIP and HRIP Acts. This plan is intended to assist staff to understand and comply with their obligations under the PPIP Act. Advice and support is available from the Privacy Contact Officer for each NSW Health organisation.

IMPLEMENTATION

Principal Officers should ensure that:

- Staff are aware of their obligations under the legislation
- staff are aware of this Privacy Management Plan
- Staff receive appropriate training and guidance on privacy matters
- The mandatory requirements for privacy training are sent out in the in Privacy Manual for Health Information
- Privacy Contact Officers for each Health Organisation are responsible for:
    - Delivering training to staff on privacy matters including
    - Conducting internal reviews where requested
    - Providing advice and assistance to staff to assist with staff compliance with the PPIP Act.

All staff are responsible for:

- Awareness of, and compliance with the Privacy Management Plan when dealing with personal information

- Identifying whether new projects are likely to raise privacy issues and consulting the Privacy Contact Officer for their NSW Health organisation where appropriate
- Identifying and raising privacy concerns with the Privacy Contact Officer for their NSW Health organisation when necessary.

REVISION HISTORY

Version	Approved by	Amendment notes
PD2015_036 (September 2015)	Deputy Secretary, Governance, Workplace, Corporate	Plan updated to reflect legislative changes in relation to privacy, policy changes in relation to the introduction of the Privacy Manual for Health and structural changes to NSW Health.
PD2005_554 (March 2005)	Deputy Director General	New policy

ATTACHMENT

1. Privacy Management Plan - Procedures.

Privacy Management Plan

NSW GOVERNMENT Health

PROCEDURES

Issue date: September-2015

PD2015_036

CONTENTS

1 BACKGROUND

NSW Health is responsible for managing and funding health services in a wide range of settings, from multi-purpose health centres in remote communities to large metropolitan teaching hospitals.

There are more than 220 public hospitals and health services in NSW which provide free health care to Australian citizens and permanent residents. Services provided at public hospitals may include emergency care, elective and emergency surgery, medical treatment, maternity services, and rehabilitation programs.

More detailed information about the structure of NSW Health is available on the NSW Health Website.

1.1 NSW Ministry of Health

The NSW Ministry of Health supports the executive and statutory roles of the Health Cluster and Portfolio Ministers.

The NSW Ministry of Health also has the role of 'system manager' in relation to the NSW public health system, which operates more than 225 public hospitals, as well as providing community health and other public health services, for the NSW community through a network of local health districts, specialty networks and non-government affiliated health organisations, known collectively as NSW Health.

1.2 Health Organisations

NSW Health comprises:

- A number of state-wide or specialist health services including NSW Ambulance, Health Infrastructure, HealthShare NSW,NSW Health Pathology, eHealth, Health Protection
- Fifteen NSW Local Health Districts providing health services across NSW (eight Local Health Districts covering Sydney metropolitan regions and seven covering rural and regional areas) and 2 Specialty networks (Justice Health and Forensic Mental Health Network and the Sydney Children's Hospital network)
- Pillar organisations (Agency for Clinical Innovation, Bureau of Health Information, Cancer Institute NSW, Clinical Excellence Commission, Health Education and Training Institute and NSW Kids and Families)
- Affiliated Health Organisations (St Vincent's Hospital, the Sacred Heart Hospice at Darlinghurst and St Joseph's Hospital at Auburn).

2 PRIVACY MANAGEMENT PLAN FRAMEWORK

2.1 Purpose of Privacy Management Plan

This Privacy Management Plan (the plan) is intended to provide information about how personal information is managed within NSW Health in accordance with the *Privacy and Personal Information Protection At 1998 (NSW)* (PPIP Act). The plan provides information about how a person can access and amend their personal information and how possible breaches of privacy in relation to personal information will be managed by NSW Health.

This plan explains how **personal** information is managed by NSW Health in accordance with the PPIP Act. It must be read in conjunction with the Privacy Manual for Health Information which comprehensively sets out how NSW Health manages **health** information under the *Health Records and Information Privacy Act 2002 (NSW)* (**HRIP Act**).

The Plain aims to:

- Meet the requirements of s33 of the PPIP Act
- Demonstrate to members of the public how we meet our obligations under the PPIP Act
- Provide staff information to enable them to manage personal information appropriately and in accordance with the law
- Illustrate our commitment to respecting the privacy rights of staff and members of the public.

2.2 Key definitions

Chief Executive – the Chief Executive of a Local Health District, Specialty Network, statutory health corporation, unit of the Health Administration Corporation, or the person responsible to the governing body of an affiliated health organisation for management of its recognised establishment and services.

Collection (of personal information) - the way the information is acquired by NSW Health. This can include a written form, a verbal conversation, an online form or a photographic image.

Disclosure (of personal information) - means providing personal information to an individual or entity outside of NSW Health.

Health information – 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, and will also include personal information that is not itself health-related but is collected in connection with providing health services.

Investigative agency – any of the following: the NSW Ombudsman's office, the Independent Commission against Corruption (ICAC) or the ICAC inspector, the Police

Integrity Commission (PIC) or the PIC Inspector, the Health Care Complaints Commission, the Office of the Legal Services Commissioner.

Law enforcement agency – the NSW Police Force, the NSW Crime Commission, the Australian Federal Police, the Australian Crime Commission, the Director of Public Prosecutions, Department of Corrective Services, Department of Juvenile Justice, Office of the Sherriff of NSW.

NSW Health – refers collectively to NSW health organisations.

NSW Health organisation – For the purposes of this policy directive, a public health organisation as defined under the *Health Services Act* 1997, NSW Ambulance, Health Infrastructure, HealthShare NSW, eHealth NSW, NSW Health Pathology, any other administrative unit of the Health Administration Corporation and all organisations under the control and direction of the Minister for Health or the Minister for Mental Health or the Secretary, NSW Health.

Personal Information - information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. This includes such things as an individual's fingerprints, retina prints, body samples or genetic characteristics. Exclusions to the definition of personal information are contained in s4 (3) of the PPIP Act and includes Health Information.

Public register – a register of personal information that is required by law to be, or is made, publicly available or open to public inspection (whether or not on payment of a fee).

Privacy obligations – the information privacy principles and any exemptions to those principles that apply to NSW Health.

Staff - any person working in a casual, temporary or permanent capacity in NSW Health, including volunteers, consultants, contractors, board members and any person performing a public official function whose conduct could be investigated by an investigating authority.

* Additional relevant definitions may be found in the Privacy Manual for Health (s1)

2.3 Legislative and Policy framework

2.3.1 Relevant Legislation

Privacy Legislation

- *Privacy and Personal Information Protection Act 1998* NSW (PPIP Act)
- Privacy and Personal Information Protection Regulation 1998
- *Health Records and Information Privacy Act 2002* NSW *(HRIP Act)*
- Health Records and Information Privacy Regulation 2006.

Other Legislation

Other legislation that may also affect the application of the privacy principles includes, but is not limited to:

- *Criminal Records Act 1991* (NSW)
- *Government Information (Public Access) Act 2009* (NSW)
- *State Records Act 1998* (NSW)
- *Workplace Surveillance Act 2005* (NSW)
- *Surveillance Devices Act 2007* (NSW)
- *Ombudsman Act 1974* (NSW)
- *Public Interest Disclosures Act 1994* (NSW)
- *Telecommunications Act 1997*
- *Telecommunications (Interception and Access) Act 1979* (Cth).

2.3.2 Relevant Policy Documents

NSW Health Internal Review Guidelines

The NSW Health Internal Review Guidelines (GL2006_007) provides guidance and information about the internal review process at NSW Health organisations.

Privacy Manual for Health Information

The Privacy Manual for Health Information is a comprehensive policy document, which governs the management of health information (as opposed to general personal information), as required by the *Health Records and Information Privacy Act 2002*. The Privacy Manual for Health Information is the primary privacy policy for NSW Health, given that the core business of NSW Health involves managing a large volume of health information.

3 WHAT THIS PLAN COVERS

S33 (2) of the PPIP Act sets out the requirements of a privacy management plan. The plan must include:

- Information about NSW Health policies and practice to ensure compliance with the PPIP Act
- How staff are made aware of these policies and practices
- Internal review procedures for NSW Health
- Anything else we consider relevant to the plan.

For most organisations, the plan includes information about compliance with the HRIP Act, however for NSW Health, this information is covered in the Privacy Manual for Health.

3.1 Personal information

Personal information is defined in s4 of the PPIP Act. Essentially, personal information is information or an opinion that identifies, or could reasonably identify, an individual.

Examples of personal information include a person's name, bank account details, a photograph or a video. Personal information also includes such things as an individual's fingerprints, retina prints, voice recordings, body samples or genetic characteristics.

A person's identity may be apparent where neither the name nor a photograph is involved, but the information about the person is such that it could not be referring to anyone else.

Section 4(3) excludes certain types of information from the definition. The most significant exceptions are:

- Information contained in a publicly available publication
- Information about an individual's suitability for public sector employment
- Information about people who have been dead for more than 30 years
- Information about an individual contained in a public interest disclosure
- A number of exceptions relating to law enforcement investigations.

Section 4A excludes ***health information*** from the definition of personal information.

Some examples of information which is NOT personal information include: recruitment records and referee reports, as well as information that is published or available on the internet. The PPIP Act also excludes certain information that may be held in connection with some activities authorised under different legislation.

For detailed information about information excluded from the definition of personal information, consult *ss 4(3)* and *4A of PPIPA* or contact the Privacy Contact Officer for your NSW Health organisation.

3.2 Health information

For guidance on the management of health information in NSW Health, refer to the Privacy Manual for Health Information.

Health information is excluded from the PPIP Act, and instead governed by the *Health Records and Information Privacy (HRIP) Act 2002*. It is defined in section 6 of the HRIP Act to include personal information or an opinion about:

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

There are 15 Health Privacy Principles set out in Schedule 1 of the HRIP Act which govern health information.

4 PERSONAL INFORMATION HELD BY NSW HEALTH

The functions of NSW Health are established primarily under the *Health Services Act 1997* and the *Health Administration Act 1982*. Given the diversity of functions across NSW Health organisations, the range of personal information held is wide-ranging.

Some of the types of personal information held by NSW Health are discussed below.

4.1 Personal information provided during enquiries

Across NSW Health, staff receive many different types of enquiries about issues in NSW Health. Enquiries are made by phone, email, in writing and in person.

People may provide NSW Health staff with personal information when they contact a NSW Health organisation with an inquiry. This could include names, contact details, opinions, health conditions and illnesses, family relationships, housing or tenancy information, work history, education and criminal history.

NSW Health decides what level of personal information is appropriate to be collected during enquiries on a case- by case basis. Sufficient information will be collected to accurately record the management of the matter. In the majority of cases, the information will be health information, which is governed by the HRIP Act and the Privacy Manual for Health. Personal information will be collected, used and stored in compliance with the PPIP Act.

4.2 Employee records

For various reasons, such as leave management, workplace health and safety and operational requirements, NSW Health keeps staff records including:

- Documents related to the recruitment process
- Payroll, attendance and leave records
- Banking details and tax file numbers
- Training records
- Workers compensation records
- Workplace health and safety records
- Records of gender, ethnicity and disability of employees for equal opportunity reporting purposes
- Medical conditions and illnesses
- Next of kin
- Secondary employment
- Conflicts of interests.

This information is collected directly from employees and will be managed in accordance with the provisions of the PPIP Act.

4.3 Business records

NSW Health maintains business records which contain personal information including contact details for public officials in other government entities, as well as other third party organisations. Contracts with other government and third party entities and individuals may include personal information. This information is managed in accordance with the provisions of the PPIP Act.

4.4 Information Management Systems

NSW Health organisations use a variety of information management systems including paper based filing systems and electronic records forming part of a secure computerised database.

We follow strict rules in storing personal information in all its formats in order to protect personal information from unauthorised access, loss or other misuse.

5 HOW TO ACCESS AND AMEND PERSONAL INFORMATION

Individuals have the right to access personal information held by NSW Health. This can be accomplished in a number of ways.

5.1 Informal request

A person wanting to access or amend their own personal or health information can make an informal request to the staff member or team managing their information. This request does not need to be made in writing, but a formal application may be required. If a person is unhappy with the outcome of their informal request, they can make a formal application.

5.2 Formal Application

Each NSW Health organisation has a privacy contact officer. A person can make a formal application to the manager or unit holding the information. More complex requests relating to personal information may be made directly to the privacy contact officer for the relevant NSW Health organisation by email, fax or post. The application should:

- Include the person's name and contact details
- State whether the person is making the application under the PPIP Act or the HRIP Act
- Explain what personal or health information the person wants to access or amend
- Explain how the person wants to access or amend it.

The person managing the request will aim to respond to the formal application within 20 working days. They will contact the applicant to advise how long the request is likely to take, particularly if it may take longer than expected.

If the applicant thinks NSW Health is taking too long to deal with the request, we encourage them to contact the privacy contact officer and request an update and time frame for the matter to be dealt with. If they remain unsatisfied, they have the right to seek an internal review or make a complaint directly to the information and privacy commissioner.

5.3 Limits and reasons for refusal

We cannot charge people to lodge their request for access. But we can charge reasonable fees for copying or inspection, if we tell people what the fees are up-front.

If there is personal information about other individuals or confidential information about third parties in any records identified by our searches, then the request will be more complex to manage. Requests of this nature ought to be referred to the privacy contact officer. This will ensure that the privacy and confidentiality of other people/third parties can also be properly considered.

6 REQUEST FOR AN INTERNAL REVIEW

6.1 Internal Review by NSW Health

If a person considers that NSW Health has breached the PPIP act or HRIP act relating to their personal or health information, they may request an internal review under the provisions of the PPIP Act. A person may not request an internal review in relation to a breach of another person's privacy unless they are an authorised representative of the person whose privacy is alleged to have been breached.

Under s53 (3) of the PPIP Act, an application for an internal review must:

- Be in writing
- Be addressed to the appropriate NSW Health Organisation
- Specify an address within Australia to which a notice can be sent
- Be lodged within 6 months from when the applicant became aware of the conduct the subject of the application (however, NSW Health may consider a late application for internal review).

6.2 Internal Review Process

An application for an internal review will be dealt with in accordance with the Internal Review Guidelines. (GL 2006_007). The review will be dealt with by the privacy contact officer for the NSW Health Organisation.

The review will be completed as soon as is reasonably practical, and within 60 days from the date the application is received.

Internal reviews follow the process set out in the Office of the Privacy Commissioner NSW's internal review checklist.

When the internal review is completed, the Privacy Contact Officer will notify the applicant in writing (within 14 days) of:

- The findings of the review
- The reasons for the finding, described in terms of the IPPs and / or HPPs
- Any action we propose to take
- The reasons for the proposed action (or no action), and

- The applicant's entitlement to have the findings and the reasons for the findings reviewed by the NSW Civil and Administrative Tribunal.

We will also send a copy of that letter to the Privacy Commissioner. Statistical information about the number of internal reviews conducted must be maintained for the Department's Annual Report.

6.3 External Review by the NSW Civil and Administrative Tribunal

People may apply to the NSW Civil and Administrative Tribunal (NCAT) for an external review of the conduct which was the subject of their earlier internal review application. A person must seek an internal review before they have the right to seek an external review. Generally, a person has 28 days from completion of the internal review to seek an external review.

The NCAT has the power to make binding decisions on an external review. For more information on how to request an external review please contact the NCAT. The NCAT does not provide legal advice, however their website has general information about the process of seeking an external review.

7 HOW THE INFORMATION PRIVACY PRINCIPLES APPLY

The *Privacy and Information Protection Act 1998* sets out 12 Information Protection Principles (IPPs). NSW Health must follow these principles for collecting, storing, using and disclosing personal. Information about the application of Health Privacy Principles (HPPs) in relation to personal health information can be found in the Privacy Manual for Health Information

This section sets out the NSW Health approach to these principles. Specific applications of these principles should be built into NSW Health policies and procedures relating to collection, storage, use or disclosure of personal or health information.

There are a number of exemptions to these IPPs, which are discussed in below at s8

COLLECTION

7.1 Lawful

NSW Health organisations will only collect personal information for a lawful purpose, which is directly related to our functions or activities and necessary for that purpose.

7.2 Direct

NSW Health organisation will only collect personal information directly from the person concerned, unless they have authorised collection from someone else or the person is under the age of 16 and the information has been provided by a parent or guardian.

7.3 Open

NSW Health organisations inform people why their personal information is being collected, what it will be used for, and to whom it will be disclosed. We tell people how

they can access and amend their personal information and the consequences if they decide not to give their personal information to us.

7.4 Relevant

NSW Health organisations ensure that personal information is relevant, accurate, is not excessive and does not unreasonably intrude into the personal affairs of people.

STORAGE

7.5 Secure

NSW Health organisations store personal information securely, keep it no longer than necessary and destroy it appropriately. We protect personal information from unauthorised access, use or disclosure

ACCESS AND ACCURACY

7.6 Transparent

NSW Health organisations are transparent about the personal information we store about people, why we use the information and about the right to access and amend it.

7.7 Accessible

NSW Health organisations allow people to access their own personal information without unreasonable delay or expense.

7.8 Correct

NSW Health organisations allow people to update, correct or amend their personal information where necessary

USE

7.9 Accurate

NSW Health organisations make sure that personal information is relevant, accurate and up to date before using it.

7.10 Limited

NSW Health organisations only use personal information for the purpose we collected it for, unless the person consents to us using it for an unrelated purpose.

DISCLOSURE

7.11 Restricted

NSW Health organisations only disclose personal information with a person's consent, unless they were already informed that the information would be disclosed, if disclosure

is directly related to the purpose for which the information was collected and there is no reason to believe the person would object, or the person has been made aware that information of that kind is usually disclosed, or if disclosure is necessary to prevent a serious and imminent threat to any persons health and safety

7.12 **Safeguarded**

NSW Health organisations will take particular care not to disclose sensitive personal information without a person's consent. For example, information about ethnic or racial origin, political opinions, religious or philosophical beliefs, sexual activities or trade union membership. We will only disclose sensitive information without consent in order to deal with a serious or imminent threat to any person's health and safety.

8 EXEMPTIONS

Some of the exemptions to the IPPs are discussed below. Different exemptions may apply between an IPP and its equivalent HPP.

When considering whether an exemption applies, it is therefore important to determine if the information is simply personal or includes health information. If the information is health information, it is necessary to refer to the Privacy Manual for Health Information for further guidance.

When considering whether an exemption may apply to a particular situation, the wording of the exemptions contained within PPIP Act should be consulted, and guidance sought from the Privacy Contact Officer. Ss 22 – 28 of the PPIP Act detail specific exemptions to the IPPs. Common exemptions include unsolicited information (which contains personal information), personal information collected before 1 July 2000, health information collected before 1 September 2004, personal information used for law enforcement or investigative purposes, or to lessen or prevent a serious threat to public health or safety.

Under s25 of the PPIP Act, NSW Health may not be required to comply with IPP's if lawfully authorised or required to do so.

Some relevant exemptions where compliance with the IPPs may not be required include:

Collection:

- When collecting information in connection with proceedings (whether or not actually commenced) before any court or tribunal
- When collecting information during investigation or management of a complaint or a matter that could be made or referred to an investigative agency, or which has been referred to NSW Health by an investigative agency
- When compliance with the IPPs in relation to collection would prejudice the interests of the individual to whom the information relates

Use:

- When the use of the information for a purpose other than the purpose for which it was collected is reasonably necessary for law enforcement purposes

- When the use of the information is reasonably necessary to enable investigation or management of a complaint which could be made or referred to an investigative agency, or which has been referred to NSW Health by an investigative agency

Disclosure:

- When the individual to whom the information relates has expressly consented to the agency not complying with the IPPs in relation to disclosure
- When the information is disclosed by a NSW Health organisation to another public sector agency under the administration of the Minister for Health if the disclosure is for the purposes of infirming that Minister about any matter within that administration
- When the information is disclosed by NSW Health 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.
- When the disclosure is made in connection with proceedings for an offence, or for law enforcement purposes
- When the disclosure is made to a law enforcement agency for the purposes of ascertaining the whereabouts of a person who has been reported missing
- Where sensitive information is required to be disclosed for law enforcement purposes where there are grounds to believe an offence may have been, or may be committed
- When the disclosure is to an investigative agency.

8.1 Public Registers

The PPIP Act governs how NSW Health manages personal information in public registers (Part 6 – Public Registers).

Under the legislation, an agency responsible for keeping a public register must not disclose any personal information kept in the register unless satisfied that it is to be used for a purpose relating to the purpose of the register, or the Act under which the register is kept. A person applying to inspect information in the public register may be required to provide a statutory declaration as to the intended use of any information obtained.

A person whose information is contained in a public register, may request the agency responsible for the register to have their information removed from public availability on the register and not disclosed to the public.

In most cases, personal information held by NSW Health is not publicly available. However, there are some circumstances where personal information may be held on registers by NSW Health which are available to the public. For example, the Tobacco Retailer Notification Scheme, which requires Tobacco retailers to provide information

including their trading name and business address and the name and address of the owners and directors of the business.

A person who wishes to access personal information contained in a public register managed by NSW Health should contact the relevant business unit responsible for the register to discuss their request.

8.2 Public interest directions

Under section 41 of the PPIP Act, the Privacy Commissioner has made Public interest directions to waive or modify the requirement for a public sector agency to comply with an IPP. Details about Public interest directions can be found at the Information and Privacy Commission website (www.ipc.nsw.gov.au).

Public interest directions may permit NSW Health:

- To be exempt from some principles in relation to the conduct of investigations
- To be exempt from some principles when transferring enquiries to another NSW public sector agency
- To disclose personal information collected for research purposes.

Public interest directions which may be relevant to NSW health organisations include:

Direction on Information Transfers between Public Sector Agencies

This Direction covers most NSW state agencies. It was originally made on 30 June 2000. On 19 June 2015 the Privacy Commissioner renewed this Direction to commence from 1 July 2015 to 31 December 2015, or until legislative amendments are made to incorporate this Direction, whichever is earlier.

Direction on the Collection of Personal Information about Third parties by NSW Public Sector (Human Services) Agencies from their clients

This Direction replaced the Direction on the Better Service Delivery Program. It commenced on 1 July 2003 and affects some health, education, welfare, housing, juvenile justice and Aboriginal affairs agencies. On 19 June 2015 the Privacy Commissioner renewed this Direction to commence from 1 July 2015 to 31 December 2015, or until legislative amendments are made to incorporate this Direction, whichever is earlier.

Direction on Disclosures of Information by Public Sector Agencies for Research Purposes

This Direction affects most NSW state agencies. It was originally made on 28 September 2000. On 19 June 2015 the Privacy Commissioner renewed this Direction to commence from 1 July 2015 to 31 December 2015, or until legislative amendments are made to incorporate this Direction, whichever is earlier.

Direction on Processing of Personal Information by Public Sector Agencies in relation to their Investigative Functions

This Direction covers most NSW state agencies. It was originally made on 30 June 2000. On 19 June 2015 the Privacy Commissioner renewed this Direction to commence from 1

July 2015 to 31 December 2015, or until legislative amendments are made to incorporate this Direction, whichever is earlier.

Direction on Disclosures of Information by the New South Wales Public Sector to the National Coronial Information System (NCIS)

This Direction affects some health and justice agencies. On 19 June 2015 the Privacy Commissioner renewed this Direction to commence from 1 July 2015 to 31 December 2015, or until legislative amendments are made to incorporate this Direction, whichever is earlier.

9 STRATEGIES FOR IMPLEMENTATION OF PRIVACY MANAGEMENT PLAN

Effective privacy governance can improve business productivity and help to develop more efficient business processes. Effective privacy governance assists NSW Health to manage both the risk of a privacy breach and our response should one occur.

Each NSW Health Organisation will develop tailored strategies suited to the organisation to assist compliance by the Health Organisation with the requirements of the PPIP Act.

NSW Health develops policies and procedure documents to assist NSW Health Organisations to comply with the IPPs and this plan.

When staff have a role that requires access to personal information, managers have a responsibility to ensure that these staff are aware of their privacy obligations in conducting their work.

9.1 Staff Awareness

Strategies adopted by NSW Health organisations to promote general privacy awareness within NSW Health organisations may include:

- Staff are provided with access to this Privacy Management Plan and relevant resources to assists with education on privacy obligations.
- New staff members receive privacy training as part of their orientation process (this **mandatory** training requirement is set out in the Privacy Manual for Health Information)
- Privacy issues are reported annually in the Annual report
- Privacy issues are identified and addressed during development and implementation of new systems
- Privacy notices are prepared as a standard inclusion in all projects where personal information will be collected
- Provision of regular privacy training and highlighting of privacy obligations (for example during Privacy Awareness Week)
- Liaison with Privacy Contact officers at their organisation or the NSW Ministry of Health where issues or queries arise that cannot be resolved locally

- Prompt referral of requests for privacy internal review (and complaints) to the privacy contact officer at the organisation
- Proactive reporting of any identified privacy breaches or risks to the privacy contact officer.

9.2 Public Awareness

Strategies adopted by NSW Health organisations to promote public awareness may include:

- Including links to the privacy management plan and other resources on NSW Health organisation websites
- Providing copies of the plan to members of the public on request.
- Referring to the privacy management plan in privacy notices
- Telling people about the plan when answering queries about personal information
- Referring enquiries to the privacy contact officer for the NSW Health organisation where appropriate.

10 LIST OF ATTACHMENTS

1. Implementation Checklist
2. Template Confidentiality Undertaking
3. Privacy Information Sheet for Personal Information

Attachment 1: Implementation checklist

LHD / Facility:			
Assessed by:		**Date of Assessment:**	
IMPLEMENTATION REQUIREMENTS	**Not commenced**	**Partial compliance**	**Full compliance**
1.	❑	❑	❑
	Notes:		
2.	❑	❑	❑
	Notes:		
3.	❑	❑	❑
	Notes:		
4.	❑	❑	❑
	Notes:		
5.	❑	❑	❑
	Notes:		
6.	❑	❑	❑
	Notes:		

Attachment 2: Template Confidentiality Undertaking

I, ... (name), understand that while I am employed by the ..... (name of health organisation) 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 Information privacy Principles contained in the *Privacy and Personal Information Protection Act 1998* (NSW) Health Privacy Principles contained in the *NSW Health Records and Information Privacy Act 2002* (NSW) (copy of Information and 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 legislation.

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
- Privacy Management Plan for NSW Health
- Data Collections - Process for Approval of New or Modified
- Electronic Information Security Policy – NSW Health
- NSW State Digital Information Security Policy

Attachment 3: Privacy Information Sheet for Personal Information

NSW Health

NSW Health is 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.

The *Privacy and Personal Information Protection Act 1998*

The *Privacy and Personal Information Protection Act* (PPIP Act) explains how NSW State and local government agencies should manage personal information.

The PPIP Act offers the people of NSW enforceable privacy rights. It gives you the opportunity to make a complaint about a public sector agency if you feel it has misused your personal information.

What do 'Privacy' and 'Personal Information' mean?

There is no simple definition of privacy. It can mean the right to a sense of personal freedom, the right to have information about oneself used fairly, and a 'right to be left alone'. Many people confuse privacy with secrecy or confidentiality, but privacy is broader than both of these.

The fair use of 'personal information' is just one aspect of this broader concept of 'privacy'.

> *Personal information is any information or opinion about an identifiable person. This includes records containing your name, address, sex, etc., or physical information like fingerprints, body samples or your DNA.*

The 12 Rules of Personal Information Protection

The Information Protection Principles (IPPs) are the backbone of the Act, and all NSW government agencies must adhere to them unless they have a lawful exemption. They are summarised here:

Collection

1. **Lawful**
   When NSW Health collects your personal information, the information must be collected for a lawful purpose. It must also be directly related to the agency's activities and necessary for that purpose.
2. **Direct**
   Your information must be collected directly from you, unless you have given your consent otherwise.
3. **Open**
   You must be informed that the information is being collected, why it is being collected and who will be storing and using it. We should also tell you how you can see and correct this information.
4. **Relevant**
   NSW Health must ensure that the information is relevant, accurate, up-to-date and not excessive. The collection should not unreasonably intrude into your personal affairs.

Storage

5. **Secure**

Your information must be stored securely, not kept any longer than necessary, and disposed of appropriately. It should be protected from unauthorised access, use or disclosure.

Access

6. **Transparent**

   The agency must provide you with enough details about what personal information

   they are storing, why they are storing it and what rights you have to access it.

7. **Accessible**

   The agency must allow you to access your personal information without unreasonable delay and expense.

8. **Correct**

   The agency must allow you to update, correct or amend your personal information where necessary.

Use

9. **Accurate**

   NSW Health must make sure that your information is accurate before using it.

10. **Limited**

    NSW Health can only use your information for the purpose for which it was collected, for a directly related purpose, or for a purpose to which you have given your consent. It can also be used in order to deal with a serious and imminent threat to any person's health or safety.

Disclosure

11. **Restricted**

    NSW Health can only disclose your information with your consent or if you were told at the time we collected it from you that we would do so, or if it is for a related purpose and we don't think that you would object. Your information can also be used without your consent in order to deal with a serious and imminent threat to any person's health or safety.

12. **Safeguarded**

    NSW Health can only disclose your sensitive personal information without your consent in order to deal with a serious and imminent threat to any person's health or safety. Sensitive information may be about your ethnic or racial origin, political opinions, religious or philosophical beliefs, health or sexual activities or trade union membership.

What to do if you think your privacy has been breached

If your complaint is about your personal information, and a NSW Health organisation you should normally seek an Internal Review.

An Internal Review is an internal investigation that NSW Health is required to conduct when you make a privacy complaint.

Contact us

If you have questions or a complaint about the privacy of your personal information, please contact the Privacy Contact Officer for the relevant NSW Health Organisation

The following link provides the names of the Privacy Contact Officers for NSW Health: http://www.health.nsw.gov.au/patients/privacy/Pages/privacy-contact.aspx