Justice Health and Forensic Mental Health Network
PO BOX 150 Matraville NSW 2036
Tel (02) 9700 3000
http://www.justicehealth.nsw.gov.au

Privacy Management Plan

Implementation Guide to NSW Health PD2015_036 Privacy Management Plan

Policy Number	2.171
Policy Function	Leadership and Management
Issue Date	31 March 2022
Summary	This policy provides information about the management of personal information held by Justice Health and Forensic Mental Health Network.
Responsible Officer	Executive Director Corporate Services
Applicable Sites	☒ Administration Centres ☒ Community Sites (e.g. Court Liaison Service, Community Integration Team, etc.) ☒ Health Centres (Adult Correctional Centres or Police Cells) ☒ Health Centres (Youth Justice NSW) ☒ Long Bay Hospital ☒ Forensic Hospital
Previous Issue(s)	N/A
Change Summary	N/A
HPRM Reference	POLJH/2171
Authorised by	Chief Executive, Justice Health and Forensic Mental Health Network

1. Preface

Justice Health and Forensic Mental Health Network (the Network) is committed to respecting the privacy rights of its employees, patients and anyone in contact with the Network. This Privacy Management Plan provides advice on how personal information is managed in the Network, in accordance with the *Privacy and Personal Information Protection Act 1998 (PPIPA)*. This plan will help staff understand and comply with their obligations under the PPIPA.

This policy is an implementation guide and should be read in conjunction with the overarching NSW Health policy directive PD2015_036 Privacy Management Plan, and covers:

- how a person can access and amend their personal information
- how possible breaches of privacy will be managed.

For information on the privacy management of health information, staff should refer to the NSW Health Privacy Manual for Health Information. Health information is specifically excluded from the PPIPA and is governed by the *Health Records and Information Privacy Act 2002 (HRIPA).*

2. Policy Content

2.1. Mandatory Requirements

All Network staff must comply with requirements of the PPIPA and PD2015_036 Privacy Management Plan.

Advice and support is available from the Network's Privacy Contact Officer.

2.2. Implementation - Roles and Responsibilities

The Chief Executive is required to:

- Ensure this policy is communicated to, and complied with by, all staff.

Organisational Development Unit are required to:

- Report on compliance of mandatory training for the Network. Mandatory requirements for privacy training are set out in the Privacy Manual for Health Information.

Supervisors / managers are required to:

- Comply with this policy in dealings associated with the privacy of their direct report and any personal information they obtain in the course of their employment
- Notify the Privacy Contact Officer of any potential privacy/data breaches in relation to personal information of employees and any personal information they obtain in the course of their employment.

Privacy Contact Officer is required to:

- Provide advice and assistance with staff compliance of the PPIPA
- Conduct investigations of potential privacy/data breaches as per the PPIPA

Conduct internal reviews where requested and as per the NSW Health Privacy Review Internal Guidelines GL2019_015.

All Staff are responsible for:

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

3. Personal Information Held by the Network

Types of personal information held by the Network are discussed below.

3.1. Personal Information provided during enquiries

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

People may provide staff with personal information when they contact the Network 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.

The Network 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.

3.2. 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
- Declaration of criminal offences and association
- Secondary employment
- Conflicts of interest

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

3.3. Business Records

The Network maintains business records that 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.

3.4. Information Management Systems

The Network uses a variety of information management systems to store corporate records, including paper-based filing systems and electronic records management systems, such as Content Manager, providing a secure digital database.

The Network follows strict rules in storing personal information in all its formats to protect personal information from unauthorised access, loss or misuse.

4. How to access and amend personal information

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

4.1. 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. An employee can also view and amend their personal information in Stafflink via the Employee Self-Service (ESS) function.

4.2. Formal Application

A person may make a formal application to the manager or the unit/department holding the information. More complex requests relating to personal information may be made directly to the Network's Privacy Contact Officer. 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 should aim to respond to the formal application within 20 working days. They should contact the applicant to advise how long the request is likely to take, particularly if it may take longer than expected.

Applicants who think the Network is taking too long to deal with the request, can be invited to contact the Privacy Contact Officer to request an update and timeframe for the matter to be dealt with. If they remain dissatisfied, they have the right to request an internal review or make a complaint directly to the Information and Privacy Commissioner.

4.3. Limits and reasons for refusal

The Network cannot charge people to lodge their requests for access. It can charge reasonable fees for copying and inspection if people are informed of these fees upfront. The current rates are outlined in NSW Health Information Bulletin IB2019_036 Health Records and Medical/Clinical Reports – Rates.

The request may be more complex to manage if there is personal information about other individuals or confidential information about third parties in any records identified by our searches. Requests of this nature should be referred to the Privacy Contact Officer to ensure the privacy and confidentiality of other people/third parties can be properly assessed.

5. Request for an Internal Review

5.1. Internal Review by the Network

Persons who consider the Network has breached the PPIP Act or the HRIP Act relation to their personal or health information may request an internal review under the provisions of the PPIP Act. A person may not request an internal review into 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) d the PPIP Act, an application for an internal review must:

- Be in writing, using the Privacy Internal Review Application form
- Be addressed to the Network
- Specify an address in Australia to which a notice can be sent
- Be lodged within 6 months from when the applicant became aware of the conduct of the subject of the application (however, the Network may consider a late application for internal review)

5.2. Internal Review Process

An application for an internal review will be dealt with in accordance with NSW Health Internal Review Guidelines (GL2019_015). The review is typically conducted by the Network's Privacy Contact Officer, unless the officer was substantially involved in the matter relating to the complaint, including attempts to informally resolve the complaint. If this is the case, an alternative review officer must be appointed.

The review will be completed as soon as 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's internal review checklist.

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

- The findings of the review
- Reasons for the findings, described in terms of the Information Privacy Principles (IPPs) and /or Health Privacy Principles (HPPs)
- Any action the Network proposes to take
- Reasons for the proposed action (or no action)
- The applicant's entitlement to have the findings and the reasons for the findings reviewed by the NSW Civil and Administrative Tribunal.

The Privacy Contact Officer will liaise with relevant Network staff to ensure any recommended actions are undertaken and completed. This will depend on the nature of the breach and the recommendations made.

The Network will also send a copy of the review outcome letter to the Privacy Commissioner. Statistical information about the number of internal reviews conducted must be maintained for the Network's Privacy Management Annual Report to the Ministry of Health. This statistical information is reported by the Privacy Contact Officer.

For more information about the internal review process, please see the Network's Information Sheet for Privacy Internal Review

5.3. 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 that 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.

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 Privacy Contact Officer or NCAT. The Tribunal does not provide legal advice, however the website has general information about the process of seeking an external review.

6. How the Information Privacy Principles Apply

The *Privacy and Information Protection Act 1998* (NSW) sets out 12 Information Protection Principles (IPPs). The Network must follow these principles when collecting, storing, using and disclosing personal information. Information about the application of the 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 Network's approach to these principles. There are a number of exemptions to the IPPs which are discussed below.

COLLECTION

6.1. Lawful

The Network will only collect personal information for a lawful purpose, which is directly related to its functions or activities and necessary for that purpose.

6.2. Direct

The Network 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.

6.3. Open

The Network will advise people why their personal information is being collected, what it is used for, and to whom it will be disclosed. The Network will inform people how they can access and amend their personal information and the consequences if they decide not to give their personal information to us.

6.4. Relevant

The Network ensures collected personal information is relevant, accurate, not excessive and does not unreasonably intrude into the personal affairs of people.

STORAGE

6.5. Secure

The Network stores information securely, keeps it no longer than necessary, and destroys it appropriately. We protect personal information from unauthorised access, use or disclosure.

ACCESS AND ACCURACY

6.6. Transparent

The Network is transparent about the personal information we store about people, why we use the information, and people's right to access and amend it.

6.7. Accessible

The Network allows people to access their own personal information without unreasonable delay or expense.

6.8. Correct

The Network allows people to update, correct or amend their personal information when necessary

USE

6.9. Accurate

The Network makes sure that personal information is relevant, accurate, and up to date before using it.

6.10. Limited

The Network only uses personal information for the purpose it was initially collected, unless the person consents to use for an unrelated purpose.

DISCLOSURE

6.11. Restricted

The Network will 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.

6.12. Safeguarded

The Network will take particular care to not 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. The Network may disclose sensitive information without consent if permitted or required by law, such as managing a serious or imminent threat to a person's health or safety.

7. Exemptions

Different exemptions may apply between an IPP and its equivalent HPP.

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

Sections 22-28 of the PPIP Act detail specific exemptions to the IPPs. When considering whether an exemption applies to a particular situation, review the wording of exemptions in the PPIP Act, and seek guidance from the Privacy Contact Officer. 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, the Network may not be required to comply with the IPPs if lawfully authorised or required to do so.

Some examples 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 matter that could be made or referred to an investigative agency, or which has been referred to the Network by an investigative agency
- When compliance with the IPPs in relation to collection would prejudice the interest of the individual to whom the information relates.

Use:

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

- When use of the information is reasonably necessary to enable investigation or management of a complaint made or referred to an investigative agency, or referred to the Network 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 informing the Minister about any matter in that administration
- When the information is disclosed by NSW Health to any public sector agency under the administration of the NSW 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.

7.1. 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 its use is related to the purpose of the register, or the Act under which the register is kept. A person applying to inspect the 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 view and not disclosed to the public.

In most cases, personal information held by NSW health is not publicly available. However there are some circumstances personal information held on registers by NSW Health is available to the public. For example, the Tobacco Retailer Notification Scheme requires tobacco retailers to provide information including their trading name, 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.

7.2. 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 on the Information and Privacy Commission website.

8. Strategies for Implementation of the Privacy Management Plan

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

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

8.1. Staff Awareness

Strategies adopted by the Network to promote general privacy awareness include:

- All new staff members receive privacy training as part of their orientation process. This required training is completed in My Health Learning and included in the EMP 127 Local Orientation Checklist
- Privacy issues are reported in the Network's Privacy Management Annual report to the Ministry of Health. These annual reports are published on the Network's website. (www.justicehealth.nsw.gov.au)
- Privacy issues are identified and addressed during development and implementation of new systems
- Privacy resources are provided to staff via the Network's intranet including access to this plan and the Privacy Information Sheet for Personal Information.
- Liaison with the Privacy Contact Officer or the NSW Ministry of Health Privacy team where issues or queries arise that cannot be resolved locally
- Prompt referral of requests for internal review (and complaints) to the Privacy Contact Officer. The relevant contact details are:

  Email: JHFMHN-Privacy@health.nsw.gov.au
  Phone: (02) 9289 5011
  Address: C/- Health Information and Records Service
  PO Box 150
  Matraville NSW 2036

- Proactive reporting of any identified privacy breaches or risks to the Privacy Contact Officer

9. Definitions

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 provision of health services to them, or a health service provided, or to be provided, to a person. Any personal information collected for the purposes of providing health care will generally be health information, including personal information that is not itself health related, but is collected in connection with providing health services. Health information is excluded from the PPIPA. For guidance on the management of health information in the Network, refer to the Privacy Manual for Health Information.

Must

Indicates a mandatory action to be complied with.

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. Examples of personal information include a person's name, bank account details, a photograph or video, fingerprints, retinal prints, voice recordings, body samples or genetic characteristics. Exclusions to the definition of personal information are contained in s4 of the PPIPA and includes Health Information.

Should

Indicates a recommended action to be complied with unless there are sound reasons for taking a different course of action.

10. Legislation and Related Documents

Legislation	*Privacy and Personal Information Act 1998* *Health Records and Information Privacy Act 2002* *Criminal Records Act 1991* *Government Information (Public Access) Act 2009* *State Records Act 1998* *Workplace Surveillance Act 2005* *Surveillance Devices Act 2007* *Ombudsman Act 1974* *Public Interest Disclosures Act 1994* *Telecommunications Act 1997* *Telecommunications Act (Interception and Access) Act 1979*
NSW Health Policy Directives and Guidelines	PD2015_036 – *Privacy Management Plan* GL2019_015 – *NSW Health Privacy Internal Review Guidelines* Privacy Manual for Health Information