# Health Records and Information Manual for Community Health Facilities

## Table of Contents

To view any policy document as published on the Policy Distribution System click the link on the policy number in the table below

<table>
<thead>
<tr>
<th>Title</th>
<th>Document no.</th>
<th>Page no.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Management Plan</td>
<td>PD2015_036</td>
<td>1</td>
</tr>
<tr>
<td>NSW Health Privacy Internal Review Guidelines</td>
<td>GL2019_015</td>
<td>20</td>
</tr>
<tr>
<td>Electronic Information Security Policy - NSW Health</td>
<td>PD2013_033</td>
<td>30</td>
</tr>
<tr>
<td>Subpoenas</td>
<td>PD2019_001</td>
<td>47</td>
</tr>
<tr>
<td>Health Records And Medical/Clinical Reports – Charging Policy</td>
<td>PD2006_050</td>
<td>47</td>
</tr>
<tr>
<td>Consent to Medical and Healthcare Treatment Manual</td>
<td>IB2020_010</td>
<td>53</td>
</tr>
<tr>
<td>Adult-to-Adult Living Donor Liver Transplantation Guidelines</td>
<td>GL2008_019</td>
<td>54</td>
</tr>
<tr>
<td>Notification of Infectious Diseases Under the Public Health Act 2010</td>
<td>IB2013_010</td>
<td>54</td>
</tr>
<tr>
<td>Notifiable Conditions Data Security and Confidentiality</td>
<td>PD2012_047</td>
<td>58</td>
</tr>
<tr>
<td>Principles for The Management of Tuberculosis In NSW</td>
<td>PD2014_050</td>
<td>65</td>
</tr>
<tr>
<td>Aboriginal and Torres Strait Islander Origin – Recording of Information of Patients and Clients</td>
<td>PD2012_042</td>
<td>66</td>
</tr>
<tr>
<td>General Retention and Disposal Authority: Patient Records (GDA17) and Administrative Records (GDA21)</td>
<td>IB2019_015</td>
<td>77</td>
</tr>
<tr>
<td>General Retention and Disposal Authority – Original Source Records that have been copied (GA4S)</td>
<td>IB2015_052</td>
<td>78</td>
</tr>
<tr>
<td>Child Related Allegations, Charges or Convictions Against NSW Health Staff</td>
<td>PD2016_025</td>
<td>79</td>
</tr>
<tr>
<td>Photo and Video Imaging In Cases Of Suspected Child Sexual Abuse, Physical Abuse and Neglect</td>
<td>PD2015_047</td>
<td>94</td>
</tr>
<tr>
<td>Managing Misconduct</td>
<td>PD2018_031</td>
<td>127</td>
</tr>
<tr>
<td>Working With Children Checks and other Police Checks</td>
<td>PD2019_003</td>
<td>129</td>
</tr>
<tr>
<td>Non-Admitted Patient Data Collection: Classification and Code Standards for Reporting Services Provided from 1 July 2016 in a Webnap Extract Format</td>
<td>IB2016_039</td>
<td>131</td>
</tr>
<tr>
<td>Non-Admitted Patient Data Collection Transition from Webnap to Edward Reporting</td>
<td>GL2015_012</td>
<td>133</td>
</tr>
<tr>
<td>State Health Forms</td>
<td>PD2009_072</td>
<td>151</td>
</tr>
<tr>
<td>Health Care Records – Documentation and Management</td>
<td>PD2012_069</td>
<td>160</td>
</tr>
<tr>
<td>Notification of Acute Rheumatic Fever And Rheumatic Heart Disease – The NSW Public Health Act 2010</td>
<td>IB2015_057</td>
<td>174</td>
</tr>
<tr>
<td>Youth Health And Wellbeing Assessment Guideline</td>
<td>GL2018_003</td>
<td>175</td>
</tr>
<tr>
<td>COVID-19 Data Collection And Reporting Requirements NSW Health Intranet Page</td>
<td>IB2020_012</td>
<td>177</td>
</tr>
<tr>
<td>COVID-19 Data Collection Summary Advisory</td>
<td>IB2020_011</td>
<td>178</td>
</tr>
<tr>
<td>COVID-19 Wards Set Up Advice</td>
<td>IB2020_013</td>
<td>178</td>
</tr>
</tbody>
</table>

Updated as at 12/05/2020
PRIVACY MANAGEMENT PLAN (PD2015_036)

PD2015_036 rescinds PD2005_554

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 Act 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 Privacy Internal Review Guidelines (GL2019_015) 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.
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.

50(17/09/15)
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 TRANSPLANT

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 informing 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
PROCEDURE MANUAL FOR COMMUNITY HEALTH FACILITIES

- 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:

50(17/09/15)
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 assist 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

50(17/09/15)
Attachment 1: Implementation checklist

<table>
<thead>
<tr>
<th>IMPLEMENTATION REQUIREMENTS</th>
<th>Not commenced</th>
<th>Partial compliance</th>
<th>Full</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

LHD / Facility:  
Assessed by:  
Date of Assessment:  
Notes:  

50(17/09/15)
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:

50(17/09/15)
PRIVACY INTERNAL REVIEW GUIDELINES (GL2019_015)

GL2019_015 rescinds GL2006_007

PURPOSE

NSW privacy law establishes a process of internal review for handling a privacy complaint, in certain circumstances.

These Guidelines help staff navigate and comply with all legislative requirements in conducting a privacy internal review. Guidance is provided on undertaking an appropriate investigation into the privacy complaint, including conducting interviews and consultation requirements.

The Appendices include template letters and reports to provide practical assistance to staff, and a consistent approach to privacy complaint handling for NSW Health agencies.

KEY PRINCIPLES

60-day time limit

A privacy internal review must be completed as soon as practicable, and a time limit of 60 calendar days applies. The 60-day time limit starts from the receipt of the first written privacy complaint or request for privacy internal review. In exceptional circumstances, the agency may ask the applicant for an extension of time. (Sections 5.3 and 5.4)

NSW Privacy Commissioner

The NSW Privacy Commissioner must be notified of all applications for privacy internal review, provided with a draft investigation report for comment, and provided with the final report and covering letter to the applicant. (Sections 5.7 and 7.3)

NSW Civil and Administrative Tribunal

An individual who is dissatisfied with the outcome of the agency’s privacy internal review, can lodge an application for administrative review with the NSW Civil and Administrative Tribunal (NCAT). This must be lodged within 28 calendar days of receipt of the privacy internal review report from the NSW Health agency. (Section 7.1)

USE OF THE GUIDELINE

Chief Executive

The Chief Executive, or their Senior Executive delegate, is ultimately responsible for the privacy internal review process and outcome. The Chief Executive, or their Senior Executive delegate, should approve the final internal review report and letter to the applicant. (Section 3.4)

Privacy Contact Officer, NSW Health agency

Privacy internal review is normally undertaken by the Privacy Contact Officer for the NSW Health agency. Privacy internal review must be undertaken without bias, and by an officer who is neutral to the circumstances relating to the complaint. If an officer was substantially involved in the matter relating to the complaint, including attempts to informally resolve the complaint, they are unable to undertake the privacy internal review. In such case, an alternative review officer must be appointed. (Section 3.4 and 5.1)
Ministry of Health

The Privacy Contact Officer, Ministry of Health and legal officers within the Legal and Regulatory Services Branch, may assist agency staff with matters of privacy internal review.

NSW Health agencies should:
- notify relevant privacy internal review matters to the Ministry, (Section 5.5)
- seek advice and clarification from the Ministry as necessary, (throughout)
- provide the draft internal review report to the Ministry for comment, (Section 6.2)
- provide final letter and internal review report to the Ministry, (Section 6.4)
- report statistical data on privacy internal reviews in the agency’s privacy annual report (Section 7.2)

The Privacy Internal Review Guideline is available at:

61(13/12/19)
ADOPTION ACT 2000 – RELEASE OF INFORMATION (PD2016_036)

PD2016_036 rescinds PD2010_050

PURPOSE

This Policy Directive provides:

- Information regarding the rights of adopted persons and their families to access information held by Information Sources under the Adoption Act 2000
- NSW Health Information Sources with direction and guidance as to what information should be disclosed to adopted persons and their families and the circumstances in which it should be disclosed.

MANDATORY REQUIREMENTS

Each NSW Health Information Source must have effective systems and procedures in place to ensure adopted persons and their families can access information in accordance with the Adoption Act 2000 and this Policy Directive.

IMPLEMENTATION

Roles and Responsibilities

Chief Executives must ensure:

- The principles and requirements of this Policy Directive are applied, achieved and sustained
- Their medical record staff are made aware of this Policy Directive.

Medical record staff have responsibility to:

- Be aware of this Policy Directive
- Release information to adopted person and their families in accordance with this Policy Directive and the Adoption Act 2000.

BACKGROUND

About this document

The Adoption Act 2000 is administered by the Department of Family and Community Services and sets out the information to which adoptees and their families are entitled to access and the manner in which a person may access that information.

Under the Adoption Act 2000, adopted persons, adoptive parents and birth parents are entitled to access prescribed information held by an “Information Source”. An Information Source includes:

- The NSW Ministry of Health
- A public hospital under the control of a Local Health District
- A statutory health corporation
- An affiliated health organisation, and
This Policy Directive provides specific information on how information about adoptees and their families held by Information Sources should be disclosed.

1.2 Legal and legislative framework
Adoption Act 2000
Adoption Regulation 2015

2 GENERAL MATTERS

2.1 Persons making general enquiries
Telephone enquiries should be directed by switchboard to the medical records department. Persons making enquiries should be informed that the Adoption Information Unit of the Department of Family and Community Services offers services regarding past adoptions, including accessing information.

The Adoption Information Unit can be contacted on 1300 799 023 or via email at adoption.information@faes.nsw.gov.au.

Where an enquirer is seeking information held by the NSW Ministry of Health, a public hospital, a statutory health corporation or an affiliated health organisation, this Policy Directive, in conjunction with the Adoption Act 2000 should be complied with.

2.2 Search fees
An Information Source may charge a fee for disclosing information held by the Information Source. Information Sources should refer to PD2006_050 Health Records and Medical / Clinical Reports - Charging Policy in respect of the fees to be charged.

2.3 Information to be provided
Adopted persons, adoptive parents and birth parents are entitled to a variety of information held by an Information Source. This policy only deals with the release of information most likely to be commonly held by NSW Health Information Sources that is health information. If there are further records relating to the adopted person, adoptive parents or birth parents held by an Information Source, you should contact your legal advisor to determine whether the information should be released.

2.4 Proof of identity
Before any information under the Adoption Act 2000 is released to an individual, that individual should provide proof of their identity and, in cases where the individual is seeking information about another person, the individual should provide proof of their relationship to the other person, such as adoption order and birth certificate(s).
2.5 Birth Parents and presumptive fathers

In this policy, a reference to an adopted person’s birth parent includes a reference to the “presumptive father” of the adopted person. Under the Adoption Act 2000, the presumptive father of an adopted person means a man who claims to be the birth parent of the adopted person and who:

(a) Is shown on the adopted person’s original birth certificate as the adopted person’s father, or
(b) Is a person whom the Information Source is entitled to presume under any law to be the adopted person’s father.

If you are unsure whether a particular person is the presumptive father of an adopted person, you should contact your legal advisor.

In some cases, an individual man will be named as the “father” in the medical records but will not be named as the father on the adopted person’s birth certificate. In these cases, the individual man’s identifying information cannot be disclosed to any person. However, in such cases, the medical records department of the Information Source should consider providing the individual man’s details to the Department of Family and Community Services who can determine whether the man would like to exchange information with the adopted person.

2.6 General guidelines for the release of information

Under s142 of the Adoption Act, an Information Source must comply with any guidelines prescribed by the Adoption Regulation before releasing information under the Act. Under clause 105 of the Adoption Regulation, the guidelines below must be complied with.

2.6.1 Confirmation of identity

The Information Source must make reasonable inquiries to confirm the applicant’s identity and relationship to the person to whom the information relates.

2.6.2 Sensitive information

The Adoption Regulation has special guidelines in relation to “sensitive information”. Sensitive information means:

(a) Information indicating that an adopted person was conceived as a result of incest or the sexual assault of his or her birth mother, and
(b) Information indicating that an adopted person has an hereditary condition seriously affecting the current, or that could seriously affect the future, physical or mental health of the adopted person or any descendant of the adopted person, and
(c) Information that could reasonably be expected to be distressing in nature to the person receiving the information.

Before disclosing sensitive information, the Information Source must:

• Make appropriate counselling and support available to the person, and
• Check whether the birth parent’s name is entered in the Reunion and Information Register. If the birth parent’s name is entered on the Reunion and Information Register, the Information Source must not disclose the sensitive information unless the Information Source has taken reasonable steps to ascertain whether the birth parent wishes to provide the information personally.
2.7 Supply Authority

Information may only be disclosed to an individual if that individual provides the Information Source with a Supply Authority issued by the Department of Family and Community Services if:

• The adoption occurred prior to 1 January 2010, or
• The adoption occurred after 1 January 2010 where the applicant is a birth parent or non-adopted sibling.

In some cases, where a Supply Authority is required before information can be released to an individual, that individual may instead produce to the Information Source an original or amended birth certificate issued under the *Adoption Information Act 1990* prior to October 1998 by the Registrar of Births Deaths and Marriages stamped with the words “Not for Official Use”.

If the Information Source is unclear whether the Supply Authority or birth certificate is valid, the Adoption Information Unit should be contacted.

3 RELEASE OF INFORMATION

3.1 Request to access information regarding adoptions occurring on or after 1 January 2010

If an adoption took place on or after 1 January 2010, an adopted person, their adopted parents and birth parents and non-adopted siblings have rights to access information held by an Information Source, including the NSW Ministry of Health, a public hospital, a statutory health corporation or an affiliated health organisation.

3.1.1 Adopted person’s rights

3.1.1 (a) Rights to access information by an adopted person who is over the age of 18

An adopted person who is over the age of 18, and was adopted on or after 1 January 2010, is entitled to receive:

• Information regarding the adopted person’s birth details (including the time of birth and weight and length at birth) and other medical records about the adopted person, and
• Any non-identifying background information about the adopted person’s birth parents, siblings, grandparents, aunts or uncles that will give the adopted person knowledge of his or her origins.

3.1.1 (b) Rights to access information by an adopted person who is under the age of 18

An adopted person who is under the age of 18, and who was adopted on or after 1 January 2010, is entitled to receive information only with the consent of the person’s adoptive parents or the Secretary of the Department of Family and Community Services.

If the adopted person produces a written consent of their adoptive parents or the Secretary of the Department of Family and Community Services, the following information should be provided to the adopted person who is under the age of 18:

• Information regarding the adopted person’s birth details (including the time of birth and weight and length at birth) and other medical records about the adopted person, and
• Any non-identifying background information about the adopted person’s birth parent, sibling, grandparent, aunt or uncle that will give the adopted person knowledge of his or her origins.
3.1.2 **Adoptive Parents’ rights**

An adoptive parent of an adopted person who was adopted on or after 1 January 2010 is entitled to receive the following information held by an Information Source:

- Information regarding the adopted person’s birth details (including the time of birth and weight and length at birth), and
- Any non-identifying background information about the adopted person’s birth parent, sibling, grandparent, aunt or uncle that will give the adoptive parent knowledge of the adopted person’s origins.

3.1.3 **Birth Parents’ rights**

3.1.3 (a) **Rights to access information by a birth parent where the adopted child is under the age of 18**

A birth parent of a person, under the age of 18, who was adopted on or after 1 January 2010 is entitled to receive information held by an Information Source only if the birth parent produces to the Information Source a Supply Authority issued by the Secretary of the Department of Family and Community Services authorising the disclosure of the information. Where a birth parent provides such a Supply Authority, the birth parent is entitled to receive the following information, subject to any conditions in the Supply Authority, held by an Information Source:

- Any non-identifying background information about an adopted person or his or her adoptive parents that will give the birth parent knowledge of the adopted child’s life, and
- Birth details of the adopted person (including the time of birth and weight and length at birth).

If the birth parent does not have a Supply Authority, information can be released if the head of the Information Source, that is the Health Secretary or the Chief Executive Officer of the relevant Information Source, is of the opinion that the information cannot be used to identify the adopted person or their adopted parents.

3.1.3 (b) **Rights to access information by a birth parent where the adopted child is over the age of 18**

A birth parent of a person, over the age of 18, who was adopted on or after 1 January 2010 is entitled to receive any of the following information held by an Information Source:

- Any non-identifying background information about an adopted person or his or her adoptive parents that will give the birth parent knowledge of the adopted child’s life, and
- Birth details of the adopted person (including the time of birth and weight and length at birth).

3.1.4 **Non-adopted sibling’s rights**

A non-adopted sibling, of a person adopted on or after 1 January 2010, is able to access any non-identifying background information held by an Information Source about the adopted person or his or her adoptive parents and adoptive family that will give the non-adopted sibling knowledge of the adopted person’s life. However, if the non-adopted sibling is under the age of 18, information can only be released with the written consent of the non-adopted sibling’s parents or the Secretary of Family and Community Services.
3.2 Request to access information regarding adoptions occurring before 1 January 2010

If an adoption took place before 1 January 2010, an adopted person, their adopted parents and birth parents have rights to access information held by an Information Source, including the NSW Ministry of Health, a public hospital, a statutory health corporation or an affiliated health organisation.

3.2.1 Adopted person’s rights

3.2.1 (a) Rights to access prescribed information by an adopted person who is over the age of 18

An adopted person who is over the age of 18, and was adopted before 1 January 2010, is entitled to receive information held by an Information Source only if the adopted person produces to the Information Source a Supply Authority issued by the Secretary of the Department of Family and Community Services authorising the disclosure of the information. Where the adopted person provides such a Supply Authority, the adopted person is entitled to receive the following information, subject to any conditions in the Supply Authority, held by an Information Source:

- Any relevant non-identifying information that is held by an Information Source about the physical and intellectual attributes, educational and vocational qualifications, social and cultural background, health and welfare, family and other relationships, religious beliefs, hobbies and interests of a birth parent, sibling, grandparent, aunt or uncle of the adopted person and that will give the adopted person knowledge of his or her origins, and

- Copies of medical reports of examinations of the adopted person made before the date of the adoption order.

3.2.1 (b) Rights to access prescribed information by an adopted person who is under the age of 18

An adopted person who is under the age of 18, and who was adopted before 1 January 2010, is entitled to receive information only with the consent of the person’s adoptive parents or the Secretary of the Department of Family and Community Services.

If the adopted persons produce a written consent of their adoptive parents or the Secretary of the Department of Family and Community Services, the following information should be provided to the adopted person who is under the age of 18:

- Any relevant non-identifying information that is held by an Information Source about the physical and intellectual attributes, educational and vocational qualifications, social and cultural background, health and welfare, family and other relationships, religious beliefs, hobbies and interests of a birth parent, sibling, grandparent, aunt or uncle of the adopted person and that will give the adopted person knowledge of his or her origins, and

- Copies of medical reports of examinations of the adopted person made before the date of the adoption order.

3.2.2 Adoptive parent’s rights

An adoptive parent of a child, under the age of 18, who was adopted before 1 January 2010 is entitled to receive any relevant non-information that is held by an Information Source about the physical and intellectual attributes, educational and vocational qualifications, social and cultural background, health and welfare, family and other relationships, religious beliefs, hobbies and interests of a birth parent, sibling, grandparent, aunt or uncle of the adopted person and that will give the adoptive parent knowledge of the adopted person’s origins.
3.2.3 **Birth parent’s rights**

3.2.3 (a) *Where the adopted person is over the age of 18*

A birth parent of an adopted person over the age of 18 adopted before 1 January 2010, is only entitled to receive information about the adopted person if the birth parent produces a Supply Authority from the Secretary of the Department of Family and Community Services authorising the disclosure of relevant information. If the birth parent produces such a Supply Authority, the birth parent is entitled to receive the following information, subject to any conditions in the Supply Authority, held by an Information Source:

- Any relevant information that is held by an Information Source about the physical and intellectual attributes, educational and vocational qualifications, social and cultural background, health and welfare, family and other relationships, religious beliefs, hobbies and interests of an adopted person or his or her adoptive parent and that will give the birth parent knowledge of the adopted child’s life after adoption
- Birth details (including the time of birth and weight and length of the person at birth), and
- Copies of medical reports and examinations of the adopted person made before the date of the adoption order.

3.2.3 (b) *Where the adopted person is under the age of 18*

A birth parent of an adopted person under the age of 18 is only entitled to receive information about the adopted person if the birth parent produces a Supply Authority from the Secretary of the Department of Family and Community Services authorising the disclosure of relevant information. If the birth parent produces such a Supply Authority, the birth parent is entitled to receive the following information, subject to any conditions in the Supply Authority, held by an Information Source:

- Birth details (including the time of birth and weight and length of the person at birth), and
- Copies of medical reports and examinations of the adopted person made before the date of the adoption order.

If the birth parent does not have a Supply Authority, information can be released if the head of the Information Source, such as the Chief Executive Officer of the relevant Information Source, is of the opinion that the information cannot be used to identify the adopted person or their adopted parents.
## 4 ATTACHMENT 1: IMPLEMENTATION CHECKLIST

<table>
<thead>
<tr>
<th>LHD / Facility:</th>
<th>Date of Assessment:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessed by:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IMPLEMENTATION REQUIREMENTS</th>
<th>Not commenced</th>
<th>Partial compliance</th>
<th>Full compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notes:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notes:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notes:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notes:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notes:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notes:</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
ELECTRONIC INFORMATION SECURITY POLICY - NSW HEALTH (PD2013_033)

PD2013_033 rescinds PD2008_052.

PURPOSE

NSW Health is committed to the provision of appropriate levels of security across all of its information systems. Health information systems containing personal information are acknowledged as having particular security requirements, and are explicitly addressed in this policy.

This policy is based on a number of key principles. These are:

- NSW Health’s major objective is the provision of health care services underlined by the overall welfare of the people it treats.
- All personal health information will be securely managed and that privacy and confidentiality will be preserved. The community must be confident NSW Health observes this principle.
- All other critical and sensitive information will also be securely managed and privacy and confidentiality maintained.
- Personnel have a responsibility for the security and maintenance of critical and sensitive information including personal health information.
- Providing information security education and developing awareness for all people dealing with electronic information is an integral part of maintaining adequate protection over that information.
- The release of information will comply with relevant and current state and federal legislation.
- The implementation of information security controls to mitigate the risks to sensitive information without impacting the timely provision of those services.
- It is also the responsibility of all NSW Health personnel and their contractors to be aware of and comply with the requirements of the NSW Health Privacy Management Plan (PD2005_554).

Please refer to Sections 2 & 3 of the Electronic Information Security Policy which provide further guidance on the policy.

MANDATORY REQUIREMENTS


- **Confidentiality** – to uphold authorised restrictions on access to and disclosure of information including personal or proprietary information.
- **Integrity** – to protect information against unauthorised alteration or destruction and prevent successful challenges to its authenticity.
- **Availability** – to provide authorised users with timely and reliable access to information and services.
- **Compliance** – to comply with all applicable legislation, regulations, Cabinet Conventions, policies and contractual obligations requiring information to be available, safeguarded or lawfully used.
- **Assurance** – to provide assurance to Parliament and the people of NSW that information held by the Government is appropriately protected and handled.
To meet the above requirements and provide appropriate assurance, implementation guidance is included as Appendix A of the policy.

IMPLEMENTATION

This policy covers security requirements for NSW Health information including electronic personal health information.

This policy applies to all employees, contractors and other persons who, in the course of their work, have access to information (including electronic personal health information) in or on behalf of the NSW public health system.

Please refer to the Section 4 titled ‘Scope’ of the Electronic Information Security Policy for implementation and scope of policy requirements.

Where access is granted to information held by the public health system for research or other purposes, the person or organisation granted access must, under the conditions of access, also be required to comply with the terms of this policy.

Compliance with this policy and all relevant acts and regulations as they relate to information security is mandatory for management, personnel and all persons handling electronic information, whether directly or indirectly involved in client service delivery.

All personnel and organisations referred to above should be aware of their legislative confidentiality obligations and that the breach of those obligations may result in prosecution and the imposition of a penalty or disciplinary actions.

1. Introduction

This document is Version 3.0 of the “NSW Health Information Security Policy” (PD2005_314).

The first version of this policy was issued on 8 July 2003 as Circular 2003/47 and published as a Policy Directive (PD2005_314) on 27 January 2005. The policy was developed following extensive consultation with a wide range of stakeholders, including significant input from clinicians.

The Second version of this policy was issued on 15 September 2008 as Premiers Memorandum M2007-04 and published as a Policy Directive (PD2008_052).

Publication of New Versions has become necessary for the following reasons:

- The applicable national standards relating to information security have changed (the new standards are AS/NZS ISO/IEC 27001:2006 and AS/NZS ISO/IEC 27002:2006);
- Government policy has been updated accordingly and the actions required of agencies in achieving the Government’s objectives have changed. The updated policy is stated in Ministerial Memorandum [http://arp.nsw.gov.au/ofis-2015-05-nsw-government-digital-information-security-policy];
- The relevant NSW Health policies concerning the privacy of personal information have been updated. The updated policy is the “NSW Health Privacy Management Plan” (PD2005_554);
- As per scheduled periodic review cycle.
1. Information Security Policy Statement

NSW Health is committed to the provision of appropriate levels of security across all of its information systems. Health information systems containing personal information are acknowledged as having particular security requirements, and are explicitly addressed in this policy.

This policy is based on a number of key principles. These are:

- NSW Health’s major objective is the provision of health care services underlined by the overall welfare of the people it treats.
- All personal health information will be securely managed and that privacy and confidentiality will be preserved. The community must be confident NSW Health observes this principle.
- All other critical and sensitive information will also be securely managed and privacy and confidentiality maintained.
- Personnel have a responsibility for the security and maintenance of critical and sensitive information including personal health information.
- Providing information security education and developing awareness for all people dealing with electronic information is an integral part of maintaining adequate protection over that information.
- The release of information will comply with relevant and current state and federal legislation.
- The implementation of information security controls to mitigate the risks to sensitive information without impacting the timely provision of those services.

3. Privacy Statement

All public sector agencies in NSW, including the public health sector, are required to comply with the Privacy and Personal Information Protection Act 1998 and the Health Records Information Privacy Act 2002, which set out a series of rules designed to protect the privacy of personal information, including personal health information, in NSW.

It is the responsibility of all NSW Health personnel and their contractors to be aware of and comply with the obligations imposed by the Act.

It is also the responsibility of all NSW Health personnel and their contractors to be aware of and comply with the requirements of the NSW Health Privacy Management Plan (PD2005_554).

These documents list the relevant NSW Health Policy Directives, other NSW Health and government policies and the relevant laws. It is the responsibility of all NSW Health personnel and their contractors to be aware of and comply with the obligations imposed by these policies and laws.

---

1 In the context of this document the term NSW Health includes all NSW Health organisations. The NSW Health organisations are: Local Health Districts (including public health units, public hospitals and Community Health Centres)/Chief Executive Governed Statutory Health Corporations, Board Governed Statutory Health Corporations, Affiliated Health Organisations – Health Administration Corporation (including HealthShare), Dental Schools and Clinics, NSW Ambulance Service, and the NSW Ministry of Health.

2 All unclassified information should be treated as “For Official Use Only” information.
4. Scope

This policy covers security requirements for NSW Health information including electronic personal health information.

“Electronic information” is information that is electronically created, processed, held, maintained and transmitted by NSW Health. It also refers to information held electronically for or on behalf of other government agencies or private entities.

“Personal health information” is personal information which concerns a person/client’s health, medical history or past or future medical treatment. It also includes other personal information collected in the course of providing a health service or information collected in relation to donation of human tissue.

“Personal information” is 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 be reasonably be ascertained from the information or opinion.

Any identifiable information is subject to this policy.

This policy applies to all information created, processed, held, maintained or transmitted by the NSW Health information or communication infrastructure. This policy shall apply to all information held for, or on behalf of, other government agencies or private entities.

Information systems refer to any information or communication infrastructure used by NSW Health and all personnel that work with it, including computer hardware and software, to create, process, hold, maintain or transmit electronic information.

For example:
- file, database and communication servers;
- computers and/or devices whether connected to a network or stand-alone (notebooks, terminals, tablets, smart phones, storage devices etc.);
- NSW Health mainframes and mid-range computers;
- devices used to store or transmit electronic data (USB storage, switches, wireless access points, etc.);
- providers of information services for NSW Health, government agencies or private entities that have been granted access rights to NSW Health information systems.

This policy applies to all employees, contractors and other persons who, in the course of their work, have access to information (including electronic personal health information) in or on behalf of the NSW public health system. This includes but is not limited to:
- providers of health services such as doctors, nurses, case managers, visiting medical officers (VMO’s) etc.;
- providers and allied health personnel;
- ambulance officers;
- administrators, clerical and service personnel;
- support staff;
- technical, research, scientific and laboratory personnel;
- auditors;
- interpreters;
• volunteers;
• Students;
• Consultants;
• temporary and contract personnel;
• external custodians of information owned by the department.

The policy applies to:
• NSW Health organisations;
• non-government organisations receiving funding from the department where compliance is included in the terms of their funding agreement;
• private hospitals and day procedures centres treating public patients/clients on a contractual basis, where the contract includes requirements for compliance with NSW Health policies;
• personnel of Health Professional Registration Boards (excluding medical, Dental and Pharmacy boards).

Where access is granted to information held by the public health system for research or other purposes, the person or organisation granted access must, under the conditions of access, also be required to comply with the terms of this policy.

Compliance with this policy and all relevant acts and regulations as they relate to information security is mandatory for management, personnel and all persons handling electronic information, whether directly or indirectly involved in client service delivery.

All personnel and organisations referred to above should be aware of their legislative confidentiality obligations and that the breach of those obligations may result in prosecution and the imposition of a penalty or disciplinary actions.

5. Information Security Requirements

The use of information and information systems is an integral part of most NSW Government activities. Electronic information assets are critical in agencies operations and are key element in delivering trustworthy government services. The security threats to information assets are increasing. The government has a duty to safeguard its large information holdings and must provide credible assurance that it is doing so. In 2001 Cabinet recognised these trends and directed that all agencies were to appropriately protect electronic information. In 2006, the document ‘People First – A new direction for ICT in NSW’ reaffirmed the importance of information security.


1. Confidentiality – to uphold authorised restrictions on access to and disclosure of information including personal or proprietary information.
2. Integrity – to protect information against unauthorised alteration or destruction and prevent successful challenges to its authenticity.
3. **Availability** – to provide authorised users with timely and reliable access to information and services.
4. **Compliance** – to comply with all applicable legislation, regulations, Cabinet Conventions, policies and contractual obligations requiring information to be available, safeguarded or lawfully used.
5. **Assurance** – to provide assurance to Parliament and the people of NSW that information held by the Government is appropriately protected and handled.

Agencies and shared services providers should adopt the following Core Requirements of the Digital Information Security Policy (DIS Policy):

1. Implement an Information Security Management System as set out in the Digital Information Security Policy;
2. Comply with the minimum controls as set out in the Digital Information Security Policy;
3. Certify the ISMS implementation where applicable;
4. Nominate a Senior Responsible Officer to represent the organisation in the Digital Information Security - Community of Practice where applicable; and
5. Provide attestation to compliance with policy if applicable.

To meet the above requirements and provide appropriate assurance, implementation guidance is included as appendix A.

Management must ensure that the implementation of information security is aligned with the organisation’s goals. This will be an important aspect for management to consider as it addresses the requirements specified by the national standards. While these standards specify particular practices to safeguard electronic information, these practices must not be adopted without regard for the organisation’s actual risk profile and business objective(s).

Guidelines should be developed where requirements specified by the standards need to be amended to meet the specific requirements of NSW Health. Not all the controls described in the standard will be relevant to every situation, nor can they take account of local environmental, budgetary or technological constraints, or be present in a form that suits every potential user in an organization.

The risk management approach allows for the tailoring of the controls to the situation. The National Standards AS/NZS ISO 31000 Risk management - Principles and guidelines, (or subsequent versions) should be used in implementing this approach.

6. **National Standards**

The national standards for an Information Security Management System (ISMS) are:

- AS/NZS ISO/IEC 27001:2006 Information technology – Security techniques – Information security management systems – Requirements; and

Both have been formally adopted unchanged as Australian & New Zealand standards and the previous standard 17799 has been renumbered as 27002. The standards are reviewed and updated about every 3 years and compliance is always to be to the current editions. Certification is to AS/NZS ISO/IEC 27001 and certifiers must be accredited by an accreditation body authorised by a national government.
The security standards are management standards and there are synergies between information security management and other management standards such as AS/NZS ISO 9001 Quality Management Systems or ISO/IEC 20000 Information technology - Service management (ITIL). It is strongly recommended that agencies that have or are seeking compliance with other management standards reduce their implementation effort by using the same management system infrastructure for compliance with different standards.

7. Roles and Responsibilities

The main objective of NSW Health is to deliver high quality care. The availability of reliable and accurate information is a key factor in the delivery of care. Clearly defined roles and responsibilities assist in the proper protection of the information assets of NSW Health.

Management (CEs or their delegates)
Management commitment to information security is demonstrated by ensuring that:
- this policy and other associated policies are implemented;
- an information security risk management system is established;
- adequate resources are allocated to policy implementation.

The CIO NSW Health
The CIO NSW Health is responsible for the management of the information security policy, procedures and guidelines.

Data/Business/Information Owners
The Data or Information Owners have the responsibility for defining the corporate information requirements and data governance policies which include development of standards and requirements for security, retention and disposal of corporate information for their information assets. They are responsible to also manage the risks to their information assets regardless if they have outsourced ICT or are sharing the risks with service providers.

Data Custodians
The Data Custodian has the responsibility for establishing and maintaining an acceptable level of data protection, for managing the disclosure of data, for ensuring that the data is used in accordance with the reasons for which it is collected and that the data is complete, of acceptable quality and is available to authorised users.

System Administrators
System administrators need to know and follow acceptable procedures for granting/revoking access, identifying and resolving known vulnerabilities, and monitoring system access. They are responsible for development of practices and procedures to support the policy and ensure compliance with the security requirements of information owners.

IT Technical and Support Staff
IT Technical and Support Staff are charged with ensuring the correct and secure configuration of systems such as servers, networks, firewalls and routers. Systems developers and maintenance staff are responsible for delivering reliable software. Technical staff should understand the business use and risks associated with the technologies being used so that security solutions match the criticality and sensitive nature of the systems. They are responsible for development of practices and procedures to support the policy and ensure compliance with the security requirements of information owners.
Users
Users of agency electronic information play an important role in overall electronic information security planning and risk management process. The effective participation of users requires a certain culture, as well as education. The culture must be supported by management directives, an education program and demonstrable support for the protection of electronic information. Users must be aware of their responsibilities with regards to Information Security and Privacy. Users have a role in identifying and reporting security concerns and incidents to management for investigation and review.

Third Party Businesses and Organisations, Consumers and Other Agencies
The growing existence of inter-connected networks requires the extension of the ‘boundaries’ of an agency. Agency executive management must ensure that third parties understand Information Security requirements and ensure that adequate security controls are in place in their own environment. All third parties must adhere to NSW Health and agency policy and procedures.

Independent Reviewer/Audit
The role of independent reviewers and auditors is to assess the effectiveness and efficiency of implemented controls, assess whether controls are being adhered to, and to check compliance against policy and legislative requirements. Review and audit reports should be noted by executive management and remedial action taken, if appropriate.

Policy Maintenance
This policy shall be reviewed by the NSW Ministry of Health and their delegates to ensure that it remains relevant and up to date with NSW Health business objectives and accurately reflects any changes in legislation or business practices that affect the security of electronic information including electronic personal health information, either directly or indirectly.
8. Appendix A – Implementation Guidelines

Intention and Principles
Technological advancement has provided significant benefits within Health and NSW Government; it has also equipped malicious users with more advanced means and tools to obtain unauthorised access to information. Any information system usage or implementation may be a target for a range of serious threats, including computer based fraud, espionage, sabotage, vandalism and other forms of systems failure or disaster. This may result in risk of data loss/leakage from accidental/malicious unauthorised access, misuse, misappropriation, modification or destruction of information and information systems that may impact service delivery. Moreover, sharing of information for business reasons, using new applications and inter-connected resources, increases the threat of information theft, loss and exposure to breaches.

Considering all the above threats, NSW Health intends to implement a structured and consistent approach to address information security risks within NSW Health. The intention is that all NSW Health agencies operate a comprehensive information security management system that meets their business-orientated security needs. This system is to comply appropriately with the national standard for such systems. Appropriateness is determined by the risks to the agency’s information assets and the potential ‘business’ implications of those risks. To provide assurance to stakeholders, including partners in government or business, the main part of the Information Security Management System (ISMS) is to address the risks based on priorities.

The principles for implementing information security are:
• Managing risks to information assets is the basis for selecting and operating information security countermeasures and controls;
• Information security countermeasures and controls are implemented and operated as elements of an Information security management system that is planned and controlled through effective management processes; and
• The cost of information security countermeasures and controls must be proportionate to the risks to information assets.

Risks and Threats
An information security risk is the combination of the likelihood and consequences of a potential information security incident or event. Information security risks arise from threats that may affect information assets in a way that adversely impacts information security objectives:
• Threats usually exploit vulnerabilities in information systems and the people that use them;
• Threats may originate internally or externally, they may be accidental or deliberate, malicious or well-meant and have human, technical or environmental sources;
• The motives behind malicious or criminal threats vary widely and will, in part, depend on how information assets can be exploited for unauthorised purposes;
• The potential value of unauthorised use of information is an important consideration and may indicate the likelihood of a threat; and
• Unacceptable information security risks are those that the ‘business’ cannot tolerate.

The key to managing information security risks in an agency is to understand the agency’s information assets, their ‘business’ significance and active involvement of the information owners in managing security of their information.

An information asset has a ‘business’ owner, ‘business’ purpose and ‘business’ value. Asset value includes both its legitimate value and its value to unauthorised users, as well as its importance to the ‘business’ and wider consequences of a security incident.
Generally an information security incident could have one or more of the following ‘business’ consequences:

- Loss of financial or material assets by agency or public - may include losses through theft or fraud, rectification costs, legal liabilities, other unbudgeted costs or lost entitlements. Losses will usually be a consequence of an information integrity failure but confidentiality or availability failures may create opportunities for loss or illegitimate gain.
- Injury or death of public or staff - could be the result of confidentiality, integrity or availability failures. If the consequences are a direct result of an ICT failure (e.g., in a real-time control system) then that system is ‘safety critical’ and appropriate methods must be applied to it.
- Inconvenience or distress to public or staff - may be a direct or secondary consequence of an event, e.g., a temporary financial loss may cause inconvenience and distress. Could arise from confidentiality, integrity or availability failures.
- Damage to standing or reputation of the Government, an agency or person, including the confidence or morale of stakeholders in a service or agency. It may be lost through confidentiality, integrity or availability failures. Treatments may include publicity campaigns to rebuild reputation or confidence and these have financial costs.
- Assist an offence or regulatory breach, hinder investigation or enforcement - may directly impact law enforcement or regulatory operations. Crime or regulatory avoidance may threaten confidentiality, integrity and availability elsewhere and have other consequences.
- Degrade the capability to deliver services internally or externally - a loss of operating capability is most likely from loss of information integrity or availability. The period required for a failure to become significant will depend on the nature of the information affected and the extent of operating dependency on it. Loss of capability may also cause regulatory non-compliance, adverse effects on stakeholders and loss of control over activities.

**Approach**

The overall objective of a management system is to ensure that current information security risks are properly identified and effectively and efficiently managed. This emphasises that information security is a management issue and a matter of information and communication technology (ICT) governance, not merely a technical problem. Deploying appropriate technical measures is necessary but insufficient to ensure continuing information security. When identifying possible threats a broad ‘business’ approach must be taken to the value of an agency’s information. This approach must consider at least agency, government and public perspectives.

Identification and assessment of the main risks enables suitable management arrangements and key policies to be established. These provide the information security management framework. Once this framework exists critical risks can be assessed more thoroughly and other risks considered. With management arrangements in place appropriate security measures, including procedures and processes, can be planned, adapted or implemented.

**Access Control**

Access control is one of the most important countermeasures in ensuring that individuals are restricted to information on a need-to-know basis and protect corporate information from unauthorised access. This concept is known as the principle of least privilege. Controls and standards for logical access should be detailed, comprehensive, and effective.

Access to NSW Health information assets will be granted based on the business need for such access. To maintain effective control over access to information, the various information asset owners should conduct a regular review of access rights.
User registration should be authorised and ensure that unique user identifier is assigned to all users. Passwords used for authentication must be kept secret and should align with appropriate password policies and standards for the agency.

No group or shared credentials and accounts are allowed for interactive login. User ID’s should be unique to each user to ensure audit and control over permissions. The information services director or their delegate may make an exception to this under appropriate circumstances.

Users are accountable for actions performed using their user ID’s.

The allocation and use of access privileges should be appropriately managed and restricted. Privileges should be assigned following the principle of least privilege access control and approved by the relevant information asset owner.

**Backup & Storage Media Handling**
Backup of data and information is required to maintain the integrity and availability of information processing and communication services.

A backup/restore strategy and procedures shall be developed for that purpose to ensure that such information is available in line with business requirements.

Storage media should be appropriately protected and managed based on the classification of information contained on that media.

Usage of personal storage media such as external storage devices is in accordance with the Use and Management of Misuse of NSW Health Communications System [PD2009_076](#).

All storage media which contains information classified “For Official Use Only or Sensitive” or higher should be disposed of securely and safely by, or on behalf of, the asset owner when the media is no longer required. This should be in compliance with the State Records Authority disposal and retention requirements.

**Business Continuity Management**
All NSW Health agencies should develop a business continuity plan for all the high risk and critical business functions. These plans should be periodically tested and regularly maintained.

**Clear Screen and Clear Desk**
Users should ensure that unattended equipment has appropriate protection. Computer screens should be locked when unattended and users should shut down or logoff the machines when not being used.

Users should maintain clean and secure storage and work areas and ensure sensitive documents are secured appropriately. Sensitive documents and information should not be left unattended.

All documents which are no longer required can be disposed of in a secure fashion. This should be in accordance with State Records Authority and any other disposal regulation or applicable policy.

All non-public documents when printed or scanned should be cleared from printers or scanners, as soon as practical, especially if they are classified as for official use only, sensitive or higher.
Confidentiality Agreements
Confidentiality or Non-Disclosure Agreements (NDA) for protection of “for official use only”, “sensitive” or higher classifications - NSW Health information should be signed before granting access to contractors and third parties.

Cryptographic Controls
Based on the risk profile of information systems appropriate cryptographic controls should be used. Cryptographic controls will be deployed and managed as directed by the regulations governing any such usage.

To maintain the security and integrity of the cryptographic keys and their underlying infrastructure, processes and procedures should be developed and documented to avoid risk exposure to information assets.

Electronic Messaging
Electronic messaging such as email can lead to accidental or deliberate disclosure of information to unauthorised users. For this purpose, the Management and Misuse of NSW Health Communications Systems (PD2009_076) Policy Directive should be adhered to by users of the email system.

Sending information that is classified as ‘sensitive’ or higher to the destinations external to the NSW Health should be encrypted using approved encryption technologies, in accordance with local laws and regulations. Communication standards such as email, FTP, telnet, Mobile SMS, instant messaging and web traffic (HTTP) are not considered secure and should be avoided.

Equipment Security
Only authorised equipment can be connected to NSW Health networks and equipment. This includes mobile devices, modems, PDAs, wireless access points, portable storage devices, CD/DVD burners and printers.

Where possible, equipment should be named and labeled as per a standard naming convention.

Fixed equipment such as servers, networking equipment and desktop computers belonging to NSW Health shall only be removed with proper authorisation. Procedures shall be used to secure equipment used outside of NSW Health premises.

All equipment should be maintained in accordance with the recommended service specification and should be disposed securely when no longer required.

Hardcopy Information
The primary focus of these guidelines is on electronic information. In practice the boundary between hard and softcopy is seldom clear-cut from a security perspective because of transformation between them. However, the inherent characteristics of the different media mean that the risks are different.

Generally, the integrity and confidentiality of hardcopy information is less vulnerable to large-scale loss but the difficulty of maintaining hardcopy “backups” can make the availability of this type of information more vulnerable to disasters. It is not the intention that agencies review and update the security measures for all their existing hardcopy information. However, improved physical security for electronic information assets will often improve the security of hardcopy information. Further guidance is given in Information Classification and Labelling Guidelines http://arp.nsw.gov.au/sites/default/files/DFS%20C2013-5%20Information%20Classification%20and%20Labelling%20Guidelines.pdf
Human Resources/Personnel - Security
Recruitment and selection processes for personnel, contractors, vendors and contingent workers will be undertaken to ensure adequate background, reference and criminal record assessments. Adequate induction and ongoing training should be provided taking into account the sensitivity of the position, and the classification of information they have access to.

Documented processes managing the change or termination of employment will be followed.

ICT Operations
Controls shall be introduced in networks to segregate groups of information services, users and information systems based on the sensitivity of the information. NSW Health networks should provide segregation between internal and external networks.

Access to network equipment should be restricted to authorised personnel only.

All changes to the ICT environment should be approved through formal change management practices.

Information Asset
Narrowly defined, electronic information assets are the data and software; owned by, licensed, leased or entrusted to an agency. It may be at rest or in transit within an agency’s systems, or being communicated to an external party. An extended definition includes hardware, networks and intangibles such as reputation, goodwill, trust, staff morale and productivity. It may be appropriate to deal with the intangibles as possible consequences of security incidents affecting other information assets.

Each information asset has an owner or custodian within the agency. The ICT group may be the ‘owner’ of ICT infrastructure. However, business information is ‘owned’ by business units. These units are responsible for ensuring that the risks to their information assets are realistically assessed and appropriately treated in accordance with Government and agency policies, etc. The appropriate level of management must formally accept any residual risks to information assets.

Acceptable usage of information assets are broadly outlined in Use & Management of Misuse of NSW Health Communications Systems, PD2009_076.

Interconnection of business and health information systems
Adequate measures should be developed and documented to ensure only approved and authorised interconnection of the NSW Health information systems with other government agencies and any third parties.

Mobile Computing, Tele-working and Remote Access
The use of mobile computing facilities and devices should be strictly governed and controlled. All the mobile computing devices should be adequately secured utilising technologies such as encryption and pass or PIN codes. Where a device is lost or stolen the relevant Information Services department or equivalent should be notified to ensure at-risk services are suspended immediately.

Mobile users should ensure that assets like tokens/laptops/smart devices and mobile phones are not left unattended and visible in public places such as airports, cafes and the back seats of motor vehicles where the risk of theft is higher. Users working remotely should also consider their environment, and take steps to ensure that equipment and information is appropriately secured from theft or disclosure to unauthorised persons.
Tele-working uses communications technology to enable staff to work remotely from a fixed location outside of their branch site location, also known as Remote Access. Remote access should be appropriately authenticated (use of multi-factor authentication is recommended) and connectivity should be protected by approved controls.

**Monitoring and Logging**
Access of NSW Health networks and resources shall be granted to only those entities who agree on consent of monitoring. Adequate logging mechanism shall be deployed to record user activities, exceptions, and information security events. Logs should be kept for the appropriate retention period to assist in future audit and access control monitoring. These logs should be protected from any accidental or deliberate modification.

The correct setting of computer clocks is important to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases such as forensic investigations. Systems clocks shall be synchronised for accurate recording to a common time source.

**Outsourcing**
Agencies that outsource any of their electronic information operations retain ownership of and responsibility for their information assets. These agencies should maintain an inventory of the external/third-party service providers and any agency’s ISMSs must include these assets if they are in scope.

Agency policies, etc., are to define clearly the detailed security responsibilities of the agency and of the provider of outsourced services affecting the agency’s information assets. These will be reflected in contracts and service level agreements with service providers, including mechanisms to ensure they can be modified to reflect changing risks. The goal is to ensure there are no gaps or ambiguities between the ISMSs of the two parties.

Regular reviews of the outsourced services and operations shall be conducted to identify the changes or improvements to the provision of services. Such reviews should also assess ongoing access requirements and compliance to the NSW Health policies.

Generally, agencies are to require the certification of outsourced service providers’ ISMS’s to the national standard.

Agencies that have outsourced will still require their own compliant and certified ISMS, even when they have no residual ‘insourced’ ICT. Subject to risk assessment, the outsourcing agency’s ISMS Statement of Applicability will focus on the non-technical aspects of their information security environment. This will ensure that the agency has effective measures for the control of their information assets and the use of assets provided by the outsourcer.

Small agencies that function as units of larger ones or are supported by secretariats or staff from larger agencies should be treated as part of the larger agency for information security compliance and certification purposes. Their inclusion should be noted in the larger agency’s Statement of Applicability.

**Physical Security**
NSW Health agencies should ensure adequate physical security is applied on all information processing facilities. The selection and design of information processing premises should take into account the possibility of damage from fire, flood, explosion, accidents, malicious intent, and other forms of natural or man-made disasters.
In addition, all Health agencies should identify and maintain an inventory of physical locations/facilities especially where business critical/sensitive assets are hosted. Delivery and loading areas shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorised access.

Access to sensitive information and information processing locations/facilities is restricted to authorised persons only. An audit trail of access should be maintained especially when access to facilities where sensitive information is located.

**Protection against Malicious code including Mobile Code**
Software and information processing facilities are vulnerable to the introduction of malicious software. Appropriate controls should be implemented to detect and prevent the introduction of malicious software, such as computer, viruses, worms, Trojan horses, root-kits, spyware, and other malware. Users must not disable or interfere with these controls.

**Publicly Available Electronic Information**
Release of electronic information to the public or service provider should be approved by the relevant branch authority and/or Communications Department.

**Reporting Security Incidents & Managing Contacts**
To reduce the business consequences and to take appropriate action against all security concerns and incidents should be reported to senior management. Consistent and repeatable processes should be adopted to address security weaknesses and events across NSW Health.

The health agencies should maintain contacts with authorities and special interest groups for liaison on operational issues. Examples of some authorities and interest groups are:
- Fire and Rescue Department
- Law Enforcement authorities
- NSW Ministry of Police and Emergency Services
- State Emergency Services (SES)
- Telecommunications Service Providers
- Electricity/Energy Service Providers
- Internet Service Providers
- Digital Information Security Community of Practice
- AUSCERT
- Defense Signals Directorate
- Specialist industry forums and groups

**Separation of Development, Test and Operational Facilities**
The level of separation between production, testing and development environments needs to be considered to prevent operational impact to services. Testing and development environments should be separated from production (operational) facilities.

Use of production data in test and development environments should be carefully controlled, and where possible, sensitive information should be removed before being utilised for testing purposes.

**Security Requirements in Systems and Applications**
The design and/or implementation of new applications and systems should take into account the security requirements and objectives of the agency. These requirements should include consideration of the classification of the information to be maintained or managed by these systems or applications.
Requirements should also take in to account information retention and business continuity requirements.

Changes to applications and systems should also take into consideration the information security requirements.

**Software licensing and use**

Only authorised software should be used. Any exceptions should be authorised from appropriate Information Services Director or their delegate. All software should be used in accordance with specified license or copyright terms and conditions. Unlicensed software shall not be installed for any reason.

**Technical Vulnerability Management**

Sensitive information systems should be subject to periodic vulnerability assessment. Adequate assessment and penetration testing processes should be used to identify the level of risk exposure for other Information systems due to these vulnerabilities. Vulnerabilities and system patches should be prioritised for remediation commensurate with the risk to the NSW agency’s information systems.

Technical audit and assessments reports should be considered sensitive and protected to prevent any possible misuse or exploit.

**Time Scale and Resources**

Agencies are to achieve the Government’s information security objectives as soon as possible. Progress will be monitored through a security status framework. Achievement of the objectives is marked by appropriate certified compliance with the standards and continuance of certification.

Information security, like physical security, is a routine function in which all staff has some role. Agencies are to act economically by making maximum use of their internal resources. Training may be necessary in some agencies. Agencies are also strongly encouraged to share security knowledge and resources. In some agencies external resources may be needed to advise, mentor inexperienced security staff and provide expert review of risk assessments and security plans.

**Online Financial Transaction**

All financial transactions carried out in the public domain or network should deploy the APRA and PCI-DSS recommended controls to protect the systems from fraudulent activity and unauthorised disclosures and modifications. This is in accordance with current regulatory compliance standards.
SUBPOENAS (PD2019_001)

PD2019_001 supersedes PD2010_065

PURPOSE
This Policy Directive outlines legislative provisions and procedures to be followed when the Ministry of Health and public health organisations are required to produce documents in response to a subpoena.

MANDATORY REQUIREMENTS
Each NSW Health Agency must have effective systems and procedures in place in order to make sure that subpoenas issued on the agency are complied with appropriately.

IMPLEMENTATION
Roles and Responsibilities

Chief Executives must ensure that:

- The principles and requirements of this policy and attached procedures are applied, achieved and sustained.
- All staff are made aware of their obligations in relation to this Policy Directive.
- Documented procedures are in place to support the Policy Directive.
- There are documented procedures in place to effectively respond to and investigate alleged breaches of this Policy Directive.

Hospital Managers and Staff have responsibility to

- Understand the legislative requirements of a Subpoena.
- Provide only the documents which are requested under the schedule of the subpoena.
- To be aware of whether any claim for privilege over the documents can be applied and take appropriate action.

The complete policy can be accessed at:

61(08/01/19)
HEALTH RECORDS AND MEDICAL/CLINICAL REPORTS – CHARGING POLICY
(PD2006_050)

The contents of this policy directive are to be effective from the date of issue and replaces PD2005_235 (dated 14 February 2002).

The following relates to charges for health records and medical/clinical reports that are to apply unless specific legislation specifies a lesser rate or exemption from fees. Health Services should develop local policies, which detail the content of records and reports as they relate to these charges. These policies should take into account the function of the health facility, the type of report produced and the amount of information to be provided.

Rates are advised separately via Information Bulletin.

The decision to charge for requests for health records and medical/clinical reports from researchers is a matter for local determination depending upon the type of request and possible future benefit to the health system. Such charges should be determined on a cost recovery basis.

For the purposes of this policy directive a health record is defined as a documented account, whether in hard or electronic form, of a client/patient’s health, illness and treatment during each visit or stay at a health service (and includes a medical record).

Charges relating to categories A, B and C (below) are taxable supplies (ie subject to GST) unless deemed GST – free under the provisions of the ‘A New Tax System (Goods and Services Tax) Act 1999’ (GST Act). The criteria to be followed by the Area Health Services/Hospitals in assessing the GST status are advised in the GST section of this circular. Please note that where the service is determined as being ‘GST-free’ the rates as advised by Information Bulletin apply. Where the GST free test is not satisfied the service is therefore a taxable supply (subject to GST) and the rates as advised by Information Bulletin are to be grossed-up by 10%.

A CHARGES FOR MEDICAL/CLINICAL REPORTS apply based on the following categories:

1. Preparation of a medical report by a medical practitioner appointed to or employed by the health institution/hospital requiring no further examination of the patient. This applies to the treating medical practitioner or a medical practitioner who has not previously treated the patient.

2. A report made by a treating medical practitioner appointed to or employed by the health institution/hospital where a re-examination of the patient is required.

3. A report made by a medical practitioner appointed to or employed by the health institution/hospital who has not previously treated the patient where an examination is required.

4. Preparation of a report by an allied health professional, other than a medical practitioner, appointed to or employed by the health institution/hospital.

22(1/07)
B OTHER CHARGES apply based on the following criteria:

1 (a) Charges for access to clinical notes requested by a patient/client, or by a person acting on behalf of the patient.

A patient/client can apply for access to their own personal health information held by a public health organisation, by contacting the medical records department for that organisation. In addition, the Freedom of Information Act 1988 and the Health Records and Information Privacy Act 2002 provide a statutory right for individuals to apply for access to information held about them.

These laws also allow for other persons to apply for access to a client/patient’s personal health information. A person can apply for access on behalf of the patient/client with their consent, such as a solicitor, interpreter or employer. Alternatively, where the patient lacks the capacity to consent, or is deceased, a person who is the authorised representative for the patient/client can apply for access to the patient/client’s personal health information.

NB. Further details are contained in NSW Privacy Manual for Health Information.

Copies of clinical notes supplied in response to the above requests may typically include, as a minimum: patient registration/front sheet, consent to treatment, discharge summary, referral/transfer letters, ambulance report, continuation notes, operation reports (including anaesthetists and nursing reports), radiology and pathology reports, and nursing care plan. Where additional information is held by a hospital but not routinely released, the person making the request should be made aware that such additional information exists but has not been supplied. A further request for such additional information should be considered as forming part of the original request and no additional charge (other than photocopying, where appropriate) should be raised.

(b) Charges for information requested by an insurer.

Health facilities should not provide clinical notes or photocopies of notes to the insurer, but may supply a “Medical Report” or “Summary of Injuries” (Section A or C) if provided with a Statutory Declaration signed by the claimant on the insurer’s claim form in respect of Compulsory Third Party (CTP) insurance or a declaration signed by the claimant on the insurer’s claim form in respect of Workers Compensation Insurance. Such reports should only provide information relevant to the claim. This will necessitate the insurer detailing the nature of the claim. Health facilities will be required to exercise their judgement in determining what is relevant information. A photocopy of the CTP Statutory Declaration is acceptable irrespective of the date of signing.

If clinical notes, or part of the clinical notes, are requested by an insurer, the insurer should be requested to provide written consent from the patient stating that the patient:

- agrees to allow the insurer to have a copy of all or part of the clinical notes and
- the patient is aware that clinical notes, or part of the clinical notes, will inevitably include confidential medical information, which is irrelevant to the claim.

In the absence of clearly documented written consent, as detailed above, hospitals are not required to provide clinical notes to insurers.
The charge applicable in respect of 1(a) and 1(b) (above), which includes search fee, photocopying charges, labour costs, administrative charges and postage, is based on the following criteria:

- A set fee for the provision of a copy of the medical record, or part thereof, eg continuation notes, pathology reports, charts. (Maximum eighty pages.)
- An additional per page rate in excess of eighty
- An additional charge at cost recovery for the provision of other material (eg reproduction of X-rays, audiovisual tapes, copies of photographs & operation footage contained on DVD’s).

Where a patient wishes to access her/his records under the *Freedom of Information Act*, the requirements of that Act (including charges) apply.

2 **Search Fees** - Other than requests made by a party concerned with a patient’s continued treatment or future management.

The search fee should be charged:

- for searching for the health record, irrespective of whether the health record is found. If however, the Patient Master Index (PMI) or other indexes showed that the patient was treated in that health institution but the record cannot be found because it has been destroyed, misplaced or lost, the fees should be refunded in full;
- where the applicant subsequently advises that a report/record is no longer required, or where a thorough search has ascertained that the patient has never attended that health institution for that particular episode of illness;
- for information on date or time of birth, including requests from the Registry of Births Deaths and Marriages in relation to enquiries on hospitals to verify birth details;
- for Motor Accident and Work Cover medical certificates completed at other than time of consultation;
- **NOTE** - The search fee is a component of the fees charged for the preparation of reports, summaries or the production of health records required by subpoena, ie additional fees should not be charged on top of those for the preparation of reports, summaries and the production of health records required by subpoena.

The fee covers processing time, which includes time for locating the information, decision-making and consultation where necessary.

C **SUMMARY OF INJURIES** - charges apply based on the following:-

“Summary of Injuries” - this is generally requested by Compulsory Third Party Insurers for patients whose fees are covered by the Bulk Billing Agreement.

The “Summary of Injuries” should include:

- Identifying information (name, date of birth, medical record number)
- Date of first attendance,
- Whether patient was admitted. If so, specify dates,
- Positive findings on examination,
- Level of consciousness, if documented,
- Diagnosis, if known.

A standard form letter may be appropriate.
If a discharge summary, or appropriate correspondence that provides this minimum information, is available at the time of the request, a copy of this may be sufficient. Should further information be required, the appropriate report charge as applicable to Section A or B should be raised. There is no requirement to provide the full clinical notes to third party insurers.

The purpose of the “Summary of Injuries” in relation to the bulk-billing agreement is to establish that the admission occurred as a result of a motor vehicle accident.

If the information contained in the “Summary of Injuries” is insufficient or unavailable and a medical practitioner (or other treating health professional, where appropriate) is required to prepare a report, charges for a medical report (or report by a treating health professional) should be raised.

Health Information Managers should consult with the requesting solicitor/insurer/other party to determine which is required before a fee is raised or report is prepared.

**Goods and Services Tax (GST) in relation to categories A, B & C (above).**

In relation to categories A, B & C above the fees/charges set by NSW Health that are taxable supplies or that Health Services are to consider for GST implications are as follows:

- Where revenue derived from the preparation of Clinical Reports is in the context of the Medical Officers Rights of Private Practice the service is to be regarded as a taxable supply.
- Where the income derived is treated as public hospital revenue, consideration is to be given as to whether it satisfies GST-free status under section 38-250 of the ‘A New Tax System (Goods and Services Tax) Act 1999’ (GST Act).

ie. Supplies are GST-free if:
- the charge is less than 50% of the GST inclusive market value of the supply; or
- the charge is less than 75% of the cost to the supplier of providing the supply.

- NB. Further details are contained in section 3.3 (pages 22 to 24) of the “NSW Health – Finance and Commercial Services – Tax Reform – GST Manual” which is available on the NSW Health Intranet.
- All Area Heath Services need to ensure that documentation/systems exist to compare the costs (including overheads) of providing health records and medical reports, and being able to assess the GST status as detailed above.
- Where the service is determined as being ‘GST-free’ the rates advised by Information Bulletin apply, or
- Where the GST free test is not satisfied the service is therefore a taxable supply (subject to GST) and the rates advised by Information Bulletin are to be grossed-up by 10%.

**D HEALTH RECORDS REQUIRED TO BE PRODUCED BY SUBPOENA**

This refers to the retrieval of all the information required by the schedule noted on the subpoena and forwarding it to Court.

Charges apply based on the following:
1. where at least 5 working days notice is given for the production of the record to Court
2. where less than 5 working days notice is given
plus a photocopying charge per page as advised by Information bulletin.

- Multiple requests on a subpoena should be charged on a fee-per-patient basis.
- In a situation where no record is found, it is appropriate to raise a Search Fee for each record, particularly in situations where incorrect details are given or “blanket” subpoenas are issued and considerable time is spent in locating the record. However, if the PMI or other indexes shows that the patient was treated in that health institution but the record cannot be found because it has been destroyed, misplaced or lost, the search fee should not be charged.
- Charges under this category are not subject to GST as they are ‘out of scope’ under a Division 81 Determination.

Reference should also be made to PD2010_065 headed ‘Subpoenas’, which outlines legislative provisions and procedures to be followed when public health organisations are required to produce documents on subpoena.

E ADMINISTRATIVE PROCEDURES

1 Policies and procedures regarding access to health records and disclosure of personal information should be made in accordance with the NSW Privacy Manual for Health Information.

2 Applicants should be asked to put all requests in writing and to provide as much information as possible. A patient’s solicitor should include consent by the patient for access to personal records as detailed in the Information Privacy Code of Practice.

3 Where the original of a health institution’s health record leaves the institution (eg health records being tendered to a Court under subpoena), a copy of those records should generally be made beforehand and kept in the institution. Charges for photocopying should be charged at the appropriate per page rate as advised by Information Bulletin. This charge does not apply to Coroner’s or Complaints Unit cases.

4 Charges should be collected in advance, where appropriate. For government departments, reimbursement may be sought subsequently from the relevant department or authority. Even where health records are required to be produced by subpoena, payment should still be sought in advance. It is emphasised that a hospital or organisation is expected to comply in due time with the requirements of a subpoena. Non-compliance may result in contempt of Court, which is punishable by fine or in certain cases imprisonment.

5 It may be decided that an examination of the patient (by either the treating medical practitioner or a medical practitioner who has not previously treated the patient) is required. Under such circumstances, the applicant should be asked to pay the balance of the money for the higher fee before proceeding with the request.

6 Fees collected are to be recorded as revenue in the General Fund.

7 Where there are disputes regarding fees or the amount of information, attempts should be made to resolve the matter between the parties involved. This would normally involve the Chief Health Information Manager and/or the General/Medical administration of the health facility.

F CIRCUMSTANCES UNDER WHICH A CHARGE SHOULD NOT BE RAISED

1 When the request has been made by a party concerned only with the patient’s continued treatment and/or future management, no charge should be raised (eg where a medical practitioner requests information from a health institution to assist him/her with that patient’s treatment);
2 The GIO or EML as Managers, Treasury Managed Fund or solicitors acting for the GIO or EML in such matters, in respect of claims for workers compensation for employees of Public Hospitals, Public Psychiatric Hospitals (former 5th schedule hospitals), the NSW Ambulance Service and the NSW Department of Health. Health facilities should ensure that solicitors acting for the GIO or EML specify in writing that this is the case;

3 Medical Services Committees of Inquiry established by the Commonwealth Government for purposes of detecting fraud and controlling over servicing;

4 The Department of Community Services or the Police in respect of children suspected of being abused, or of a parent of a child so suspected;

5 The completion of medical certificates at the time of consultation - no charge should be made as the forms for motor accident and WorkCover certificates are in the nature of a certificate and not a report. If not completed at the time of consultation, a search fee may be raised.

G CIRCUMSTANCES UNDER WHICH CHARGES SHOULD BE RAISED

In all cases where the conditions in Section F have not been met including:

1 When medical reports/records are requested by individuals, solicitors, insurance companies, health professionals and government departments (with the exception of those indicated in Section F) for purposes other than the patient’s continued treatment or future management.

2 The Department of Veterans’ Affairs and Centrelink for the purpose of pension/benefits assessment;

3 Interstate Health Authorities in respect of the eligibility of candidates for appointment to the relevant Public Service.

4 NSW Compulsory Third Party Insurers, in respect of a “Summary of Injuries”. (Refer to Section C).

5 Release of information under the NSW Adoption Information Act 1990. Charges should be raised in accordance with PD2010_050 or any document subsequently amending its provisions.

ENQUIRIES

- pertaining to the level of charges and GST implications refer to the latest Information Bulletin on ‘Charges for Health Records and Medical/Clinical Reports and the “NSW Health – Finance and Commercial Services – Tax Reform – GST Manual” (available on the NSW Health Intranet site) respectively or contact Trevor Smith, Finance and Business Management on (02) 9391 9158.

- pertaining to access of information contact Legal Branch on 9391 9606.

- pertaining to records management policy should be referred to the Informatics Senior Project Officer on (02) 9391 9155.


- Health Records and Medical/Clinical Reports

- Fees under the Public Health Act

- Fee for Cremation Certificates issued by Salaried Medical Practitioners of Public Hospitals
CONSENT TO MEDICAL AND HEALTHCARE TREATMENT MANUAL

The manual rescinded PD2005_406 – notified under IB2020_010


The Consent Manual provides operational guidance and procedures to support compliance with the NSW law on obtaining consent to medical and healthcare treatment from patients or their substitute consent providers.

The Consent Manual incorporates changes in legislation and NSW Health policy which impact on the legal obligations for obtaining consent to medical treatment.

The Consent Manual has been developed to achieve the following outcomes:

- assist Health Practitioners and managers in understanding the legal requirements for providing appropriate and adequate information to patients, including material risks of specific treatments, procedures and obtaining valid patient consent for such treatment / procedures to help them in discharging their legal obligations

- alert Health Practitioners and managers to their legal obligations with regard to providing treatment to patients who do not have capacity to consent

- patient consent or refusal of treatment is recorded and documented appropriately

- patient autonomy and decision making is respected and patients are provided with appropriate information relevant to their treatment.

The Consent Manual is available at:

61(26/03/20)
ADULT-TO-ADULT LIVING DONOR LIVER TRANSPLANTATION GUIDELINES (GL2008_019)

The purpose of the guideline is to provide guidance to health professionals and additional protection for prospective adult Living Donor Liver Transplantation (LDLT) donors. This guideline is aimed primarily at the jurisdictions that will endorse LDLT, the institutions that will provide LDLT, and the health professionals directly involved in this practice. To the extent that it is adopted by all jurisdictions in line with the particular requirements of their human tissue legislation, and applied in participating liver transplant units, it will promote ethical, lawful and consistent application of quality processes in provision of this complex procedure to donors, recipients and their families.

These Guidelines should be in conjunction with PD2005_406.


23(02/10)

NOTIFICATION OF INFECTIOUS DISEASES UNDER THE PUBLIC HEALTH ACT 2010 (IB2013_010)

IB2013_010 rescinds IB2012_011.

PURPOSE

Under the provisions of the Public Health Act 2010 and the Public Health Regulation 2012, doctors, hospital chief executive officers (or general managers), pathology laboratories, directors of child care centres and school principals are required to notify certain medical conditions listed on the Ministry of Health website.

NOTIFICATION MECHANISMS

- Infectious disease notifications should be directed to the local Public Health Unit, and should be initiated as soon as possible within 24 hours of diagnosis.
- In order to protect patient confidentiality, notifications must not be made by facsimile machine except in exceptional circumstances and when confidentiality is ensured.

NOTIFICATION FORMS

Doctors and Hospitals

- Doctors and hospital chief executive officers (or general managers) must notify scheduled medical conditions and provide information specified in the Doctor/Hospital Notification Form, either by telephone or in writing. The notification can be found at: [http://www.health.nsw.gov.au/Infectious/Documents/doctor-hospital-notification-form.pdf](http://www.health.nsw.gov.au/Infectious/Documents/doctor-hospital-notification-form.pdf)
- Notifications for AIDS must only include the first 2 letters of the patient’s first and last names, and date of birth. Full name and addresses are not to be included.

37(28/02/13)
Laboratories

- Laboratories must notify scheduled medical conditions and provide information specified in the Labor
  ory Notification Form, either by telephone or in writing.
- Notifications for HIV infection should only include the first 2 letters of the patient’s first and last
  names, and date of birth. Full name and addresses are not to be included.
- Laboratories carrying out confirmatory testing for HIV must notify infections directly to
  Communicable Diseases Branch. The HIV notification form can be found at:

(b) The list of notifiable diseases in Schedule 2 to that Act:
   (i) that must be notified by health practitioners providing care in hospitals to the Chief
       Executive Officer of the hospital concerned, and
   (ii) that must be notified by the Chief Executive Officer of a hospital to the Director-General
        of the Ministry of Health.

NOTIFICATION MECHANISMS

- Information on the notification of infectious diseases under the Public Health Act 2010 is detailed
- Infectious disease notifications should be directed to the local Public Health Unit, and should be
  initiated as soon as possible within 24 hours of diagnosis.
- In order to protect patient confidentiality, notifications must not be made by facsimile machine
  except in exceptional circumstances and when confidentiality is ensured.
- Disease notification guidelines and notification forms for notifiers are available at:

PURPOSE

This policy articulates the professional and legal responsibilities of all health workers to promote the health, safety, welfare and well-being of children and young people, working collaboratively with interagency partners in the shared system of child protection in NSW. These responsibilities apply whether workers are providing health care directly to children and young people or to adult clients who are parents/carers or are pregnant.

This policy informs Local Health Districts, Specialty Health Networks, other health services and health workers about the tools and resources available and the interagency arrangements in place to assist them to meet their responsibilities and provide a consistent NSW Health response to child protection and wellbeing.

MANDATORY REQUIREMENTS

Every health worker has a responsibility to protect the health, safety, welfare and wellbeing of children or young people with whom they have contact.

The legal responsibilities of health services and health workers are identified in the following legislation:

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

- Collaborate with interagency partners and comply with information exchange provisions to promote the safety, welfare and wellbeing of children and young people, including taking reasonable steps to coordinate the provision of services with other agencies;
- Meet requirements for mandatory reporting of children and reporting of young people (or classes/groups of children or young people) at suspected risk of significant harm (ROSH);
- Report unborn children where it is suspected they may be at ROSH after their birth;
- Respond to the needs of children and young people after making a report to Community Services or to the NSW Health Child Wellbeing Unit;
- Respond to Community Services’ and Children’s Court requests to provide health services and or Community Services and Police Force requests to provide medical examinations and treatment;
- Assist with Children’s Court proceedings when required.


- Meet requirements to ensure that only people with valid Working with Children Checks are engaged in child related work (where a child is under the age of 18 years).

*Ombudsman Act 1974*

- Maintain systems to prevent ‘reportable conduct’ by health workers and for reporting and responding to alleged reportable conduct involving NSW Health employees.
The policy responsibilities of health workers are to:

- Recognise and respond appropriately to the vulnerabilities, risks and needs of families, children and young people when providing any health service;
- Collaborate across NSW Health services and with interagency partners to support and strengthen families and promote child health, safety, welfare and wellbeing;
- Use the Mandatory Reporter Guide and seek assistance from the NSW Health Child Wellbeing Unit to help identify children or young people at suspected risk of significant harm (ROSH);
- Seek assistance from the NSW Health Child Wellbeing Unit and the Family Referral Services to help respond to vulnerable families, children and young people below the ROSH threshold;
- Actively seek feedback from Community Services after making a child protection report and continue to support the child, young person or family consistent with the health worker’s roles and responsibilities;
- Follow the Child Wellbeing and Child Protection - NSW Interagency Guidelines and other agreed interagency procedures when working with children, young people and families, including in relation to information exchange, High Risk Birth Alerts, Prenatal Reporting, escalation of child protection concerns, assumption of care by Community Services and out of home care health assessments;
- Collaborate in joint investigation and response to matters involving alleged child sexual assault or serious child abuse or neglect leading to criminal proceedings; and
- Participate in mandatory and/or other child protection training for NSW Health workers.

IMPLEMENTATION

Chief Executives across the NSW public health system are responsible and accountable for:

1. Ensuring that this policy and the associated Child Wellbeing and Child Protection Fact Sheet for NSW Health Workers are understood and implemented by all health workers; and
2. Enabling frontline staff to operationalise this Policy Statement in accordance with the attached Child Wellbeing and Child Protection Policies and Procedures for NSW Health.

To download the complete document please go to

38(18/04/13)
NOTIFIABLE CONDITIONS DATA SECURITY AND CONFIDENTIALITY (PD2012_047)

PURPOSE

The purpose of this policy is to provide guidance for NSW Health staff to manage the security and confidentiality of Notifiable Conditions data in any form, either unit records or aggregated form. This includes:

- Paper notification records;
- Electronic notification records;
- The Notifiable Conditions Information Management System (NCIMS);
- The Secure Analytics for Population Health Research and Intelligence (SAPHaRI); and/or
- Any other form of data that has not been approved for release in the public domain.

MANDATORY REQUIREMENTS

All NSW Health and Local Health District staff must comply with this policy when accessing, managing or analysing notifiable conditions data.

Prior to accessing notifiable conditions data, NSW Health staff must sign each page of the Notifiable Conditions Data Security and Confidentiality Policy Directive, to confirm that they have read, understood and agreed to comply with the policies, procedures and conditions set out in it.

Release of notifiable conditions data must be managed according to section 4 – Data and information release.

IMPLEMENTATION

This policy directive should be distributed to all NSW Health staff. Staff with access to notifiable conditions data must follow the procedure set out in this policy directive.

All staff with access to notifiable conditions data in any form must sign the Notifiable Conditions Data - Confidentiality and Security Agreement at Appendix 1.

1. INTRODUCTION

1.1 About this document

Notifications of Scheduled Medical Conditions made under the Public Health Act include highly confidential information. NSW Health staff from Local Health Districts and the NSW Ministry of Health with access to such information should always protect the security and confidentiality of this information.

1.2 Key definitions

This policy refers to the security and confidentiality of Notifiable Conditions data in any form, either unit records or aggregated data. This includes paper or electronic notifications, the Notifiable Conditions Information Management System (NCIMS), the Secure Analytics for Population Health Research and Intelligence (SAPHaRI), or any other form that has not been approved for release in the public domain.
2. LEGAL AND LEGISLATIVE CONTEXT

The conditions and procedures set out in this document are supplemental and subordinate to any State or Commonwealth statutes, legislation or regulations and any NSW Health policies or guidelines subsequently issued by the Director-General which relate to confidentiality and data security.

Specifically, management of confidential notification data are referred to in the following legislation:
- NSW Public Health Act 2010
- Health Administration Act 1982

NSW Health Employees with access to notifiable conditions data must also acquaint themselves with the NSW Health Records and Information Privacy Act 2002.

3. ACCESS TO SCHEDULED MEDICAL CONDITIONS DATA

3.1 Personnel

Access to notifiable conditions data for NSW Health Staff should be limited to the minimum level required to fulfil the functions of their position. Individuals requesting access to scheduled medical conditions data (and their managers) must:
- Be aware of their responsibilities with regard to information privacy.
- Undertake training on the operation of any databases or systems which they will operate to record or access personal health information in relation to notifiable conditions data.
- Complete the Confidentiality Agreement (Appendix 1) and identify the appropriate level of access according to their position and role.

3.2 Security

3.2.1 Password Security

NSW Health staff with access to databases containing information on notifiable conditions must observe the following measures in order to maintain security:
- Each individual is assigned a unique username. Access to the data will be controlled by a password. The password must be known only to the individual.
- Passwords are required to be a minimum 6 and maximum 12 characters and contain at least one numeric and at least one text character.
The individual must not record their password in any file or other electronic document, no matter where or how such a file or document is stored.

Individuals must change their passwords when requested by system administrators.

3.2.2 Electronic Security

- Access to notifiable conditions data through the NCIMS web based application is to be through individual login passwords only.
- When an individuals’ access to the notifiable conditions data is no longer required (i.e. the role of the staff member changes, or their employment by the organisation at which they worked when the Confidentiality Agreement was signed), the staff member and or manager must notify the System Administrators of their changed circumstance, so that role changes can be made or logins disabled.
- System administrators will undertake an audit of NSW Health staff with access at least twice annually.

3.2.3 Physical Security and Storage of Data

- Electronic notifiable conditions data should be password protected and stored on secured networks with appropriately restricted access, not standalone PCs.
- Where access to notifiable conditions data through the NCIMS application is required externally (outside the usual work environment), individuals must ensure that information is not downloaded or saved to a PC.
- Network hardware and any back up or copies of notifiable conditions data must be password protected and stored in a secure location.
- Hard copies of identifiable notifiable conditions data related scheduled medical conditions should be stored in locked cabinets in a secure location.
- Secure document disposal facilities must be available.
- Secure printers and faxes must be available for confidential data management.

3.2.4 Workstation Security

- Care must be taken not to leave documents containing personal health information related to notifiable conditions data on work benches or anywhere they may be visible to unauthorised people.
- Personal health information should be unloaded from computer monitors (or the screen locked) if the monitor is to be left unattended.
- These requirements also apply where notifiable conditions data is handled externally (outside the physical confines of the usual work environment).

3.3 Acceptable use of notifiable conditions data

Notifiable conditions data must only be used for official NSW Health/Local Health District business related to notification or public health action, unless authorised in writing by an appropriate officer (see section 4 - Data and Information Release).

Notifiable conditions data should not be used for personal study. Use of the data for research purposes is subject to the NSW policy directive PD2015_037: ‘Data Collections - Disclosure of Unit Record Data Held for Research or Management of Health Services’ referred to in section 4 - Data and Information Release. Where an individual holds external organisation (e.g. academic) and NSW Health/Local Health District appointments, access to notifiable conditions data must not be used for any academic or teaching purposes without prior approval.
4. DATA AND INFORMATION RELEASE

4.1 Legal context for release of data

This section should be read in conjunction with ‘Data Collections - Disclosure of Unit Record Data Held for Research or Management of Health Services’ (PD2015_037).

NSW Health staff with access to notifiable conditions data must not release, pass on or otherwise make available to third parties (where the first party is NSW Health and the second party is the notifiable conditions data user) any data, subset of data or any tables, graphs or other aggregations or manipulations of data obtained or derived from notifiable conditions data where this data or information allows the identification of individual persons, institutions, communities or organisations by any means.

NSW Health staff with access to notifiable conditions data should note that identification of individuals, communities or organisations may occur through the release of specific identifying information such as addresses, or by inference from the combination of multiple non specific or less specific data items (such date of birth plus postcode).

The authority to disclose notifiable conditions data is vested in:

a) the Director-General or his/her delegate (for identified unit record data) under the Health Administration Act 1982 and the Health Administration Regulation 2012 (subject to the conditions of that Act and Regulation).

b) The Chief Health Officer (for epidemiological data) under the Public Health Act 2010 and Health Administration Act and Health Administration Regulation (subject to the conditions of those Acts and Regulation).

There are no delegations relating to the disclosure of identified unit record notifiable conditions data under the Public Health Act.

The delegations under the Health Administration Act 1982 can be found in section 10 of the Combined Delegations Manual at http://www.health.nsw.gov.au/policies/manuals/Pages/combined-delegations.aspx

Other persons are not authorised to disclose notifiable conditions data.

4.2 Applications for release of data

Applications for release of notifiable conditions data should be made through the relevant data custodian using the appropriate form and will be assessed in accordance with PD2015_037 (Appendix 2).

Applications for the release of identified unit record notifiable conditions data for research or management of health service should be submitted to the NSW Population and Health Services Research Ethics Committee for consideration as per policy directive PD2010_055 Ethical & Scientific Review of Human Research in NSW Public Health Organisations. Available at: www.health.nsw.gov.au/policies/pd/2010/PD2010_055.html

Specific guidelines for the release of Aboriginal health information related to notifiable conditions data are required to protect Aboriginal people from the risk of identification as individuals or communities. Disclosure of Aboriginal health information must comply with the NSW Aboriginal Health Information Guidelines.
4.3 Exceptions for release of identifying data

Under the *Public Health Act 2010* (Section 130), it is an offence to disclose information obtained in connection with the Act unless the disclosure is made:

- with the consent of the person whom the information was obtained;
- in connection with the administration or execution of the Act or regulations;
- for the purposes of legal proceedings arising out of the Act or the regulations, of a report of any such legal proceedings;
- with the approval of the Chief Health Officer, or a person authorised by the Chief Health Officer, to a person specified in the approval and the information consists of epidemiological data specified in the approval;
- in any other prescribed circumstances; or
- with other lawful excuse.

4.4 Acknowledgement of use of data in publications

Where notifiable conditions data is approved for release in research or management of health services, all approvals must include a condition that data recipients agree to include a written acknowledgement of the role of NSW Health and the Centre for Health Protection in the fulfilment of any data requests and in the preparation of any report, scientific paper or on-line document (such as a World-Wide Web page). Typically the acknowledgement will appear in the covering letter, foreword or, in the case of electronic documents, as part of the introductory or top-level pages.

The source of notifiable conditions data should be attributed to the underlying data collection. For example, a graph which displays notifiable disease information derived from Notifiable conditions data should have the following attribution: “Source: Notifiable Conditions Information Management System, NSW Health”.

Where data is accessed via a secondary interface, such as SAPHaRI, the underlying data collection should be referenced along with the method of extraction: “Source: Notifiable Conditions Information Management System (Secure Analytics for Population Health Research and Intelligence), NSW Health”.

5. DURATION OF THIS AGREEMENT

The applicant agrees to be bound by the conditions of this Agreement indefinitely or until they sign a new Confidentiality and Data Security Agreement which supersedes this agreement.

The applicant is bound by this Agreement regardless of whether they continue to be an active user of the notifiable conditions data or database system and regardless of whether they remain an employee of or associated with the NSW Health or Local Health District.

LIST OF ATTACHMENTS

1. Notifiable conditions Confidentiality and Security Agreement
2. Data request template
Appendix 1

Notifiable Conditions Data - Confidentiality and Security Agreement

I, [full name of applicant], hereby

[Work phone number] [work e-mail address]

[employed as Position]

By (Name of business unit employing the person)______________________________

Agree to abide by the confidentiality and data security conditions and procedures set out in this document.

By signing this document and each page of the Notifiable Conditions Data Security and Confidentiality Policy Directive, I confirm that I have read, understood and have agreed to comply with the policies, procedures and conditions set out in it.

I undertake not to knowingly access any personal health information unless such information is essential for me to properly and efficiently perform my duties. I undertake strictly to preserve the confidentiality of this information and I understand that a breach of this undertaking will result in disciplinary action.

I acknowledge my statutory duty under Sections 22 and 23 of the NSW Health Administration Act 1982 and Section 1.90 of the NSW Public Health Act 2010, in relation to the disclosure of information. In order to fulfil this undertaking, I will not divulge any identifying, personal or health information regarding individual persons, except to authorised staff of the NSW Ministry of Health, Local Health District or other staff who require such information to carry out their medical or public health duties.

I further undertake to inform my supervisor immediately if I become aware of any breach of privacy or security relating to the information which I access in the course of my duties.

Signature of applicant ________________________________ Date: ____________

Position Title: ________________________________

Witnessed by (Name of witness): ________________________________

Signature of witness: ________________________________ Date: ____________

To be completed by Unit manager employing the applicant:

I confirm that, to properly fulfil the functions of their position, the above signed has reasonable need for access to notifiable conditions data. I also confirm that, in order to properly undertake the business of NSW Health or Local Health District, the business unit has a valid requirement for access to this data.

Manager's Name: ________________________________

Signature: ________________________________ Date: ____________

Position Title: ________________________________

Business Unit Name: ________________________________ Local Health District: ________________________________

For access to notifiable conditions data through the NCIMS application - please tick all that apply

Applicant position: Administration

intended role: Administration

immunisation staff: Data entry

Project office: Data cleaning/analysis

Public Health Nurse: Epidemiological analysis

Surveillance Officer: Outbreak response

Tuberculosis Nurse: Surge Capacity

Other (describe): ________________________________ Other (describe): ________________________________

End of Agreement

33(16/08/12)
Appendix 2

Request for Release of Notifiable Conditions Data
Request for release of notifiable conditions data by requesters external to NSW Health or Local Health District.

To be completed by person making the request

1. Person and/or agency making request:

2. Purpose for which data is sought:

3. □ Epidemiological/aggregate data       □ Unit record data
   Where unit record data are sought, please provide a copy of the NSW Population and Health Services Research Ethics Committee approval (according to PD 2012_010)

4. Description of data requested [disease/condition, fields of interest, & time period of interest]

5. What (if any) publication of data is intended?

6. Date data requested by: (allow up to 6 weeks from the date of request) _______ / _______ / _______

7. Person taking responsibility for appropriate use of data:

   Name: ___________________________    Position: ___________________________
   Organisation name: ___________________________
   Phone: ___________________________    Email: ___________________________
   Signature: ___________________________    Date: ___________________________

Fax this form to the Surveillance Manager, Communicable Diseases Branch on 02 9391 9189

NSW Health reserves the right of comment on use of data and interpretation prior to publication.

<table>
<thead>
<tr>
<th>Request Received:</th>
<th>Request Approved:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date request completed: _______ / _______ / _______</td>
<td>Date prepared by: ___________________________</td>
</tr>
</tbody>
</table>
PRINCIPLES FOR THE MANAGEMENT OF TUBERCULOSIS IN NSW
(PD2014_050)

PD2014_050 rescinds PD2008_019.

PURPOSE

This policy sets out the mandatory principles for the provision of Tuberculosis (TB) services in New South Wales (NSW).

TB Services are required to operate in accordance with this policy in conjunction with the current relevant guidelines for the prevention and control of tuberculosis in NSW, which reflect best practice for the clinical and public health management of TB.

MANDATORY REQUIREMENTS

All staff must adhere to these principles. All services related to the screening, care and management of people with active, latent, or suspected TB are available at no charge to patients within the NSW Public Health system. The treatment for people with active TB is to be administered by directly observed treatment.

IMPLEMENTATION

Chief Executives must ensure that:

- The principles and requirements of this policy are applied, achieved and sustained
- Relevant staff are made aware of their obligations in relation to the Policy Directive
- Documented procedures are in place to support the Policy Directive.

Clinicians:

- Must comply with this Policy Directive.


45(18/12/14)
ABORIGINAL AND TORRES STRAIT ISLANDER ORIGIN – RECORDING OF INFORMATION OF PATIENTS AND CLIENTS (PD2012_042)

PD2012_042 rescinds PD2005_547.

PURPOSE

The policy directive and the associated procedures document outlines the requirements for collecting and recording accurate information on whether clients of NSW Health services are Aboriginal and/or Torres Strait Islander. Aboriginal and Torres Strait Islander people are under-reported in many health related data collections in NSW. Self-report in response to the standard Australian Bureau of Statistics question about a person’s Aboriginality is the most accurate means of ascertaining whether a client is Aboriginal and/or Torres Strait islander. The standard question must be asked of all clients of NSW Health services, and the information needs to be recorded accurately according to national standards.

MANDATORY REQUIREMENTS

1. All NSW Health services are required to collect consistent and comprehensive data on Aboriginal and Torres Strait Islander health.

2. The Aboriginal and Torres Strait Islander Origin – Recording of Information of Patients and Clients: Procedures document describes the standards required for the accurate collection and recording of data.

3. The standard question seeking information about a person’s Aboriginality should be asked of all clients of NSW Health services to establish whether they are Aboriginal and/or Torres Strait Islander:

   ‘Are you (is the person) of Aboriginal or Torres Strait Islander origin?’

4. These standard response options should be provided to the clients to answer the questions (either verbally or on a written form):
   - No
   - Yes, Aboriginal
   - Yes, Torres Strait Islander
   - Yes, both Aboriginal and Torres Strait Islander

5. Asking the question:
   - Staff responsible for registering a client should ask the standard question when the client is first registered with the service.
   - The question should be asked of all clients irrespective of appearance, country of birth, or whether or not the staff know the client or their family background.
   - Clients may be asked the question directly, or asked to complete a form with the question included, and the client should answer this question themselves.
   - Specific situations related to asking the question are described in Section 2 and Section 4 of the Procedures document.

6. Recording the Information:
   - Information systems should record whether a client is Aboriginal or Torres Strait Islander using the standard categories, which are outlined in Section 3 in the Procedures document.
   - Responses to the standard questions should be coded as described in Section 3 in the Procedures document.
• A response to the standard question should be a mandatory requirement when registering or entering client details in electronic recording systems.
• Local data management systems must be able to identify those records that are coded as not stated/inadequately described which require follow-up.

7. Training in the correct and consistent recording of whether a client is Aboriginal and/or Torres Strait Islander must be delivered to all staff. See Section 5 in the Procedures document.

8. Data quality assurance and validation activities must be undertaken at the local level (Section 6 Procedures document) and by NSW Ministry of Health (Section 7 Procedures document).

IMPLEMENTATION

1. Roles and Responsibilities of NSW Health agencies:
   • Chief Executives, Health Service Executives, and Managers are responsible for the implementation of this policy and procedures at the local level.
   • All NSW Health employees are responsible for the accurate recording of Aboriginality when ever this is part of their role.

2. Roles and Responsibilities of NSW Ministry of Health:
   • NSW Ministry of Health is responsible for providing the mandatory requirements and procedures, and to support the implementation and evaluation of this policy.

3. Activity Based Funding
   With the implementation of activity based funding in July 2012, accurate and consistent recording of Aboriginality is essential for the effective application of associated weighting and will enable LHDs/SHNs to:
   • Monitor expenditure on health care against funding for Aboriginal clients.
   • Enable clinicians and managers to understand the factors contributing to cost variations including the extent to which these relate to patient complexity or differences in the way services are delivered to Aboriginal clients.
   • Make decisions about where to invest additional resources to meet increasing demand in the most cost effective way for Aboriginal clients.
   • Contribute information about costs to the national “price setter”, the Independent Hospital Pricing Authority.
   • Be appropriately funded according to the efficient pricing for treating Aboriginal patients.

1. BACKGROUND

1.1 About this document
This Policy Directive replaces Policy Directive PD2005_547 ‘Aboriginal and Torres Strait Islander Origin - Recording of Information of Patients and Clients’. This policy directive revises and updates the previous policy.

1.2 Legal and legislative framework
The ‘National best practice guidelines for collecting Indigenous status in health data sets’ (AIHW, 2010) documents the national approach for collecting and recording accurate information on whether a client is Aboriginal and/or Torres Strait Islander.
The Council of Australian Governments (COAG) National Indigenous Reform Agreement requires all jurisdictions, including NSW, to implement the National Best Practice Guidelines.

This policy and procedures document incorporate the activities outlined in the National Best Practice Guidelines. The implementation of these will ensure NSW meets their National Indigenous Reform Agreement obligations in relation to identification of Aboriginal and Torres Strait Islander people.

2. ASKING THE QUESTION

2.1 The Standard Aboriginal and Torres Strait Islander Origin Question

The following question should be asked of all clients to establish whether they are Aboriginal and/or Torres Strait Islander:

'Are you (is the person) of Aboriginal or Torres Strait Islander origin?'

2.2 The standard response options

2.2.1 Three standard response options should be provided to the clients to answer the questions (either verbally or on a written form):

- No
- Yes, Aboriginal
- Yes, Torres Strait Islander
- Yes, both Aboriginal and Torres Strait Islander

2.2.2 If the question has not been completed on a returned form, this should be followed up and confirmed with the client.

2.3 How to ask the question

2.3.1 Staff responsible for registering a client should ask the standard question seeking information about a person’s Aboriginality when the client is first registered with the service.

2.3.2 The question should be asked of all clients irrespective of appearance, country of birth, or whether the staff know of the client or their family background.

2.3.3 The question should be placed within the context of other questions related to cultural background, such as country of birth and main language spoken.

2.3.4 Clients may be asked the question directly, or asked to complete a form with the question included, and the client should answer this question themselves.

2.3.5 In some situations (such as in the case of birth and death registrations) the client will be unable to answer the question themselves. In this case it is acceptable for certain others (such as mother, father, close friend, relative, or household member) to be asked the question and to answer the question on the client’s behalf if they feel confident to provide accurate information.

2.3.6 In instances where the client is temporarily unable to answer the question, it is also acceptable for certain others who know the client well to respond on their behalf; however this response should be verified with the client wherever possible.
3. RECORDING RESPONSES

3.1 How to record responses

3.1.1 Information systems should record information on whether a client is Aboriginal and/or Torres Strait Islander using the standard national categories, which are:
1. Aboriginal but not Torres Strait Islander origin
2. Torres Strait Islander but not Aboriginal origin
3. Both Aboriginal and Torres Strait Islander origin
4. Neither Aboriginal nor Torres Strait Islander origin
9. Not stated/inadequately described
In addition databases in NSW should use the following additional category:
8. Declines to respond

3.1.2 Responses to the standard questions should be coded to the following national standards.

<table>
<thead>
<tr>
<th>Response</th>
<th>Coding Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>‘Yes, Aboriginal’ is ticked, but ‘Yes, Torres Strait Islander’ is not ticked.</td>
<td>1</td>
</tr>
<tr>
<td>‘Yes, Torres Strait Islander’ is ticked, but ‘Yes, Aboriginal’ is not ticked.</td>
<td>2</td>
</tr>
<tr>
<td>‘Yes, Aboriginal’ is ticked, and ‘Yes, Torres Strait Islander’ is ticked.</td>
<td>3</td>
</tr>
<tr>
<td>‘Yes, both Aboriginal and Torres Strait Islander’ is ticked</td>
<td>3</td>
</tr>
<tr>
<td>‘No’ is ticked</td>
<td>4</td>
</tr>
<tr>
<td>‘No’ is ticked and either/both ‘Yes, Aboriginal’, and ‘Yes, Torres Strait Islander’ is ticked.</td>
<td>1, 2 or 3</td>
</tr>
<tr>
<td>Client is capable of responding but declines to respond following prompting/follow-up</td>
<td>8</td>
</tr>
<tr>
<td>Where it is impossible for the question to be asked during the contact period</td>
<td>9</td>
</tr>
<tr>
<td>Response to the question has been left blank or is incomplete</td>
<td>9</td>
</tr>
</tbody>
</table>

(Note these categories represent national standards, with the addition of the code 8, used by NSW to identify clients who have declined to respond. In the national categories, the NSW Code 8 would be coded as 9. See Section 3.3 for further information.)

3.2 Mandatory completion

A response to the standard question on a person’s Aboriginality should be a mandatory requirement when registering or entering client details in electronic recording systems. Staff registering or entering details of a client should not be able to proceed with registration until a response has been completed.

3.3 Identifying records for follow up

3.3.1 Local data management systems should be able to identify those records that require follow up. In NSW the code 8 is used (as described in 3.1.2) to identify clients who have declined to answer, and therefore do not require follow up. Client’s coded as 9 (not stated/inadequately described) because of situations where it was impossible for the question to be asked during the contact episode, and other situations where the response was left blank or incomplete, require follow up with the client, to determine the correct code.

3.3.2 Additional categories used by NSW or in local systems for the purposes of workflow management and follow-up must be mapped to the correct national category (Categories 1, 2, 3, 4, and 9) before the data are provided to the national data custodian. In NSW, data coded as category 8 (declined to respond) must be recoded to category 9 before submission to national data custodians.

32(26/07/12)
4. IMPLEMENTING THE PROCEDURES IN SPECIFIC SITUATIONS

4.1 In the event of a birth

4.1.1 For perinatal data collections, the standard questions on whether a client is Aboriginal and/or Torres Strait Islander should be asked directly of the mother, regardless of the information separately recorded in the hospital database.

4.1.2 In NSW, information on whether the mother and the newborn baby are Aboriginal and/or Torres Strait Islander must be recorded in the NSW Perinatal Data Collection (see NSW Policy Directive PD2015_025).

4.1.3 The mother should be asked to provide the information on whether her baby is Aboriginal and/or Torres Strait Islander in addition to her own Aboriginality.

4.1.4 It should not be assumed that the baby will share the mother’s origin. In particular, if the mother does not report her origin as Aboriginal and/or Torres Strait Islander, it should not be assumed that the newborn is therefore not Aboriginal or Torres Strait Islander.

4.2 If the client is a child under 15

4.2.1 Where the client is a child under 15 years of age, the parent or guardian is asked to declare whether the client is Aboriginal and/or Torres Strait Islander on their behalf.

4.2.2 If the parent or guardian is not available, certain others may be asked to provide this information (see 2.3.4).

4.2.3 If the accompanying adult is unable to provide this information, the child’s parent/guardian should be contacted as follow-up to establish whether the child is Aboriginal and/or Torres Strait Islander.

4.3 If the client is too ill to be questioned or is unable to respond

4.3.1 When the client is unable to respond to the standard question because they are too ill, unconscious, or too ill due to psychiatric condition or dementia, in the first instance the staff member should ask the client’s carer, relative, or any other person accompanying the client (see 2.3.4).

4.3.2 The response provided by this person should be verified with the client when they have recovered sufficiently to be able to answer the questions themselves.

4.3.3 If the person accompanying the client does not know whether the client is Aboriginal and/or Torres Strait Islander, the client should be asked the question directly when they are capable of responding.

4.3.4 In the event that the person accompanying the client does not know whether the client is Aboriginal and/or Torres Strait Islander and the client does not recover sufficiently to provide this information, the answer to the standard question on Aboriginality should be recorded as a non-response.
4.4 If the client does not speak English, or cannot read or write

4.4.1 If the client does not speak English, but is accompanied by someone who can interpret for them, it is recommended that the person accompanying them is asked to translate the question and their response.

4.4.2 If there is no-one with the client who can speak English, it is recommended that an interpreter, or Aboriginal or Torres Strait Islander liaison officer (who can interpret the relevant Aboriginal or Torres Strait Islander language spoken by the client) be called to assist.

4.4.3 If a form is to be provided and the client cannot read or write, it is recommended that an appropriate staff member (e.g. an interpreter, social worker, Aboriginal or Torres Strait Islander Liaison Officer) go through the questions with the client.

4.4.4 All clients’ should be given the opportunity to respond to the standard Aboriginality question for themselves. While a client who speaks an Aboriginal language may be highly likely to be an Aboriginal person, their Aboriginality cannot be assumed; the client may be of both Aboriginal and Torres Strait Islander for example.

4.4.5 Non-English speaking clients from various cultural backgrounds should also be asked the question and given the opportunity to self-report in response to the standard question.

4.5 If the client is deceased

4.5.1 Funeral directors, undertakers, medical practitioners and coroners responsible for registering a death or assessing the cause of death must ask the next-of-kin about whether the deceased is Aboriginal and/or Torres Strait Islander. If no next-of-kin is available, then the question should be asked of the broader family. If this information is not able to be obtained from either of these sources, another person who knew the deceased well may be asked to provide this information.

4.5.2 If information on whether the deceased is Aboriginal and/or Torres Strait Islander is missing on the death registration form, the funeral director should follow up with the next-of-kin before the form is sent to the registry. Similarly, medical practitioners or the coroner responsible should attempt to complete this item before the deceased’s information is sent to the registry.

4.6 If staff are reluctant to ask the question

4.6.1 Staff should be encouraged to collect information from all clients in a professional and respectful manner, without anticipating or making assumptions about the client’s identity or about how the client is likely to react or respond to any given question. Staff should be encouraged to regard the standard question on a person’s Aboriginality as no more or less sensitive or problematic than other items of personal data routinely collected from clients.

4.6.2 All client’s, whether Aboriginal, Torres Strait Islander, or non-Aboriginal or Torres Strait Islander, have the right to self-report, rather than have their identity assumed and recorded on their behalf. To refrain from asking any client the standard question on a client’s Aboriginality is an act of discrimination which infringes upon the client’s right to respond to this question for themselves.

4.6.3 Staff should not modify the standard question in any way. The question should be asked correctly, consistently, and uniformly of all clients, using the wording precisely as stated in this policy and procedure.
4.7 If the client wants to know why they are being asked the question

4.7.1 The following provides several responses that may assist staff in explaining to clients the reasons for asking the standard question on a client’s Aboriginality:
   
   a. The question on whether a person is Aboriginal and/or Torres Strait Islander is one of several questions related to a client’s identity and demographic characteristics that are asked of all clients who attend a health service, enrol with Medicare, or are involved in the registration of a birth or death.
   
   b. The collection of information on whether a person is Aboriginal and Torres Strait Islander is necessary for government and other services to plan and deliver appropriate services for all Australians, to assess the impact of services on particular groups in the community, and to improve health care and to monitor changes in health and wellbeing over time.
   
   c. The response to this question allows service providers to ensure that Aboriginal and Torres Strait Islander clients have an opportunity to access relevant services such as Aboriginal liaison officers and Aboriginal health workers, health checks, Aboriginal and Torres Strait Islander specific immunisation considerations and PBS listings if they choose.
   
   d. Service providers cannot make assumptions about whether a person is Aboriginal, Torres Strait Islander, or non-Aboriginal and Torres Strait Islander, therefore this information can only be determined by asking the client the standard question.
   
   e. All personal information is protected by privacy law.

4.7.2 Should a client request a more detailed explanation of where the data go or the ways they are used, staff may wish to refer the client to the Australian Institute of Health and Welfare website www.aihw.gov.au or the Australian Bureau of Statistics website www.abs.gov.au.

4.8 If the client objects to the question or declines to answer

4.8.1 Where a client objects to the question or declines to answer they should be informed of their right to decline to answer the standard question on whether a client is a Aboriginal and/or Torres Strait Islander person and be advised that their level of care and access to services will not be affected if they choose not to answer the question.

4.8.2 While staff have a duty to collect and record information on whether a client is Aboriginal and/or Torres Strait Islander from all clients as correctly as possible, they are not obliged to convince a disgruntled, upset or unwilling client to respond to the question.

4.8.3 While staff have a duty, if queried, to explain to clients why this question is being asked, they are not obliged to justify the use of the standard question.

4.9 If the client chooses not to answer the question ‘correctly’

4.9.1 There may be occasions where a client is known to staff as an Aboriginal or Torres Strait Islander person yet the client chooses not to report as such in response to the standard question. Conversely there may be occasions where a known non-Aboriginal or Torres Strait Islander person chooses to report themselves as Aboriginal or Torres Strait Islander in response to this question.
Clients have a right to self-report whether they are Aboriginal and/or Torres Strait Islander and staff should therefore always record the response that the client provides; they should not question or comment on the client’s response.

4.9.2 The client’s recorded response should not be altered or annotated in any way to reflect the views of the staff member collecting the information.

4.10 If a client identifies as Aboriginal and/or Torres Strait Islander

4.10.1 Any client who self-reports as Aboriginal and/or Torres Strait Islander should be offered the services of Aboriginal liaison officers or Aboriginal health workers where available; however, the client’s choice to engage or not engage with such services should be respected.

4.10.2 Information about a person’s Aboriginality should be included on the client’s discharge summary.

4.11 If the client wishes to change personal information on their record

4.11.1 All clients should have the opportunity to confirm or update any previously recorded personal information on a regular basis, including confirmation or alteration of a record that they are Aboriginal and/or Torres Strait Islander.

4.11.2 The NSW Health Client Registration Policy (PD2007_094) describes when to update client registration details. Client/patient details, including information on Aboriginal and Torres Strait Islander origin, should be checked and confirmed or updated, as appropriate each time a client presents for a new phase of treatment.

4.11.3 Any changes to the previously recorded information on whether a client is Aboriginal and/or Torres Strait Islander should be received without comment and clients should not be required to provide a reason for changing their record.

5. STAFF TRAINING

5.1 Training in the correct and consistent collection of information on whether clients are Aboriginal and/or Torres Strait Islander must be delivered to all staff.

5.2 This training may be delivered as part of a training that focuses on overall data collection and data quality.

5.3 While it is recommended that all staff receive training in cultural safety for Aboriginal and/or Torres Strait Islander clients, such training should not be considered a pre-requisite for the collection of information on whether a client is an Aboriginal and/or Torres Strait Islander person using the standard question.

5.4 All staff must complete training requirements as outlined in the Respecting the Difference: An Aboriginal Cultural Training Framework for NSW Health (PD2011_069).

5.5 All persons responsible for collecting, recording and validating information on whether clients are Aboriginal and/or Torres Strait Islander should be able to demonstrate the following competencies:
   a. An ability to ask the standard questions Are you of Aboriginal or Torres Strait islander origin? correctly, and to correctly record responses on paper forms and/or computer systems.
b. An ability to clearly explain to clients the reason for collecting this information.
c. An understanding of why it is important to collect and record information on whether all
   clients are Aboriginal and/or Torres Strait Islander.
d. An understanding of why it is important to collect this information correctly and
   consistently, using the standard question.
e. An understanding of the voluntary nature of self-reporting a client’s Aboriginality, and of
   a client’s right to decline to answer this question or to change the information recorded.
f. Knowledge of available information and services for Aboriginal and Torres Strait
   Islander clients, and ability to convey this to clients as required.
g. Knowledge of and ability to conduct follow-up procedures for obtaining missing
   information, including whether a client is Aboriginal and/or Torres Strait Islander.

6. DATA QUALITY ASSURANCE AND VALIDATION AT LOCAL SERVICE LEVEL

For data quality assurance and validation at the local service level, local service providers must:

6.1 Review all forms and data recording systems to ensure the standard question on whether a
   client is Aboriginal and/or Torres Strait Islander is included and that coding categories are
   consistent with this policy and procedure.

6.2 Provide appropriate training, supervision and support to staff in primary data collection and
   data management roles, to ensure data items such as the item recording a client’s Aboriginality
   are collected correctly and consistently

6.3 Ensure data collection processes and systems are streamlined and user friendly for staff in data
   collection roles.

6.4 Review client intake procedures to ensure client privacy is maintained, particularly in areas
   where clients are interviewed to obtain personal information.

6.5 Ensure staff across various levels and disciplines within the service are prompted to check for
   and follow up on missing client registration details, including information on a client’s
   Aboriginality, in their contact with clients.

6.6 Establish business rules for distinguishing between ‘not stated/inadequately described’ records
   that are a result of a client’s inability to answer (and are therefore to be followed up) and ‘not
   stated/inadequately described’ records in which the client declined to answer (which do not
   require further follow up).

6.7 Establish policies and procedures for correctly following up and correctly coding records with
   incomplete information on whether a client is Aboriginal and/or Torres Strait Islander.

6.8 Establish business rules for checking information on a client’s Aboriginality against other data
   items, particularly country of birth, language spoken, and Medicare eligibility.

6.9 Monitor trends in the number and proportion of Aboriginal and/or Torres Strait Islander clients
   by comparing with the previous year’s data, to determine whether there have been any obvious
   errors in coding.

6.10 Conduct data quality surveys involving direct surveys or interviews with clients, to determine
      the consistency and accuracy of the collection of information on whether clients are Aboriginal
      and/or Torres Strait Islander and to develop estimates of under-reporting.
7. **DATA QUALITY ASSURANCE AND VALIDATION AT NSW MINISTRY OF HEALTH**

For data quality assurance and validation state-wide, NSW Ministry of Health must:

7.1 Ensure data providers are aware of the policy and procedure.

7.2 Ensure the correct business rules are applied to cope with different identifications when there are two sources of data (e.g. cause of death forms and death registrations). For example, if one data source identifies the client as Aboriginal or Torres Strait Islander, the record relating to this client should be coded accordingly.

7.3 Regularly monitor information on whether clients are Aboriginal and/or Torres Strait Islander and provide continuing feedback on data quality to local services. In particular, monitor levels of ‘not stated’ reported from local service providers to determine whether further education or assistance is required.

7.4 Regularly check that codes used for recording a client’s Aboriginality in local systems are consistent with the policy and procedures, in particular check that invalid or inappropriate codes are not being used.

7.5 Compare data for Aboriginal and Torres Strait Islander persons with variables such as country of birth, language spoken, and Medicare eligibility, and follow up with local service providers to ensure any issues are investigated.

7.6 Regularly check that local service providers have not set default values for the standard question seeking information on whether a client is Aboriginal and/or Torres Strait Islander. This would be evidenced by no reporting of records with a ‘not stated’ response to the standard question.

7.7 For each local service, compare the number and proportion of records with information indicating clients are Aboriginal and/or Torres Strait Islander with the previous year’s data to determine whether there have been any probable errors in coding.

7.8 Establish a system of review and audit of data collection processes and data quality for local service providers, including review and audit of Aboriginal and Torres Strait Islander data.

7.9 Inform the national data custodian of any events or issues that may have affected the quality of data recording whether clients are Aboriginal and/or Torres Strait Islander for a given period.

7.10 Establish a procedure for the prompt investigation and response to data validation requests from the national data custodian.

8. **MONITORING**

Monitoring of the implementation and impact of this policy directive will be undertaken by NSW Ministry of Health and Local Health Districts:

8.1 In partnership with the Australian Institute of Health and Welfare, NSW Ministry of Health conducts a biannual survey which estimates the level of correct reporting of Aboriginal and Torres Strait Islander people in NSW public hospital data.
8.2 Local Health Districts will be required to determine appropriate indicators to monitor the adherence to this policy.

9. REFERENCES

GENERAL RETENTION AND DISPOSAL AUTHORITY: PATIENT RECORDS (GDA17) AND ADMINISTRATIVE RECORDS (GDA21) (IB2019_015)

IB2019_015 rescinds IB2004/20 and IB2005_027

PURPOSE
The Board of the State Archives and Records Authority NSW has approved a revised General retention and disposal authority: Public health services - patient records (GDA17), and made a minor change to General retention and disposal authority: Public health services – administrative records (GDA 21) in line with the approval of the Functional retention and disposal authority: Provision and regulation of childcare services (FA404).

KEY INFORMATION
1. General retention and disposal authority: Public health services – patient records (GDA17)

GDA17 applies to the records of patient care provided by the NSW Health system. The authority underwent a review and was revised on 30 May 2019.

The disposal action for certain patient records has been changed as a result of the review. NSW State Archives and Records website has available the current version of GDA17 and a schedule of amendments and justifications to show where the retention periods have changed. Where they have changed the old entries in GDA17 can no longer be used as the source of legal authority for the disposal of records under the State Records Act 1998.

2. General retention and disposal authority: Public health services - administrative records (GDA 21)

GDA21 applies to records created and maintained to support the management and delivery of public health care services and programs. It was amended on 30 May 2019 to remove classes covered by FA404, Provision and regulation of childcare services. Those sections of GDA21 relating to childcare can no longer be used as the source of legal authority for the disposal of records under the State Records Act 1998.

FA404 applies to the provision of childcare services by NSW public offices including the local health districts. Refer to the NSW State Archives and Records website for the latest version of both GDA21 and FA404.

ATTACHMENTS
The authorities mentioned in this information bulletin are available from the NSW State Archives and Records website using the following links.

<table>
<thead>
<tr>
<th>Authority</th>
<th>Link</th>
</tr>
</thead>
</table>
GENERAL RETENTION AND DISPOSAL AUTHORITY – ORIGINAL SOURCE RECORDS THAT HAVE BEEN COPIED (GA45) (IB2015_052)

**IB2015_052 rescinds IB2009_064.**

**PURPOSE**

To notify the Health system that State Records Authority General Retention and Disposal Authority: *Original or source records that have been copied (GA 45)* has been issued to replace General Retention and Disposal Authority: *Imaged records (GA36)*.

GA 45 provides for the authorised destruction of original or source records that have been copied, provided that certain conditions are met.

**KEY INFORMATION**

GA 45 provides for the authorised disposal of certain State records which have been successfully copied using microfilming or digital imaging processes. In particular, it describes the circumstances and conditions under which the destruction of certain original or source records is permitted under the provisions of the *State Records Act 1998* after they have been copied.

Whereas GA36 established the conditions under which original records that had been microfilmed or imaged could be destroyed, it primarily applied to paper and excluded records identified as State archives or those required to be retained where created prior to 2000.

The main changes from GA36 to GA45 are:

- Records that are required as State archives or required to be retained in agency may now be destroyed after copying (if the conditions have been met and they do not fall within the exclusions categories) if they were created after 1980, rather than 2000.
- The scope of the authority was widened from original records copied using microfilming or digital imaging processes, to original or source records that have been copied.
- The requirement to assess all requirements for retaining originals was removed, as this condition has become less relevant due to digital copies of paper records being widely accepted.
- Additional exclusions have been included in GA 45 to cover State archives on loan from State Records and records that have high personal value to individuals who were subject to Government control.

Further information on GA45 can be accessed on the State Records website: [http://www.records.nsw.gov.au/recordkeeping/rules/retention-and-disposalAuthorities/general-retention-and-disposalAuthorities/original-or-source-records-that-have-been-copied-1/frequently-asked-questions-re-original-or-source-records-that-have-been-copied](http://www.records.nsw.gov.au/recordkeeping/rules/retention-and-disposalAuthorities/general-retention-and-disposalAuthorities/original-or-source-records-that-have-been-copied-1/frequently-asked-questions-re-original-or-source-records-that-have-been-copied)

CHILD RELATED ALLEGATIONS, CHARGES OR CONVICTIONS AGAINST NSW HEALTH STAFF (PD2016_025)

PD2016_025 rescinds PD2006_025

PURPOSE

This Policy Directive and the attached Procedures set out the mandatory requirements for managing child related allegations, charges and convictions involving NSW Health staff, which includes, for the purpose of this policy, anyone working in NSW Health, whether as a paid staff member or engaged in any other capacity, including as a volunteer, Visiting Practitioner, student attending clinical placement or anyone else appointed on an honorary or contractual basis. It also applies to staff of the NSW Ministry of Health.

Child related allegations and convictions include any alleged behaviour or criminal charges or convictions against NSW Health staff that may constitute reportable conduct, as specified under Part 3A of the Ombudsman Act 1974, where the alleged victim was under the age of 18 years at the time of the alleged behaviour; this extends to child pornography, non-work related and historical matters.

This Policy Directive includes the requirements of the Ombudsman Act 1974 and the requirements of Part 5 of the Child Protection (Working with Children) Act 2012.

MANDATORY REQUIREMENTS

All child related allegations and convictions against current NSW Health staff members must be:

- Reported to the Child Protection Helpline if there is suspected risk of significant harm relating to a child or a class of children:
  - Where there are concerns about a child that do not meet the threshold for a mandatory report, the NSW Health Child Wellbeing Unit must nevertheless be contacted.

- Reported to the NSW Police if there is alleged criminal conduct

- Notified to the employing Chief Executive (or Secretary, NSW Health in the case of NSW Ministry of Health staff), including where the person works in a different NSW Health organisation to where the allegation has been identified

- Notified to the NSW Ministry of Health via a Reportable Incident Brief (RIB) by the Chief Executive (or delegated person) within 24 hours

- Investigated (unless the facts are clear and uncontested), risk managed and findings made, consistent with the processes in the NSW Health policy on Managing Misconduct (or Government Sector Employment Act in the case of NSW Ministry of Health staff) and the requirements of this policy

- Notified to the NSW Ombudsman using Part A of the Ombudsman’s Notification Form as soon as possible and in any event within 30 days of the matter being brought to the attention of the NSW Health organisation (unless the matter falls outside of the definition of reportable conduct)
  - The NSW Ombudsman must also be notified of the outcome using Part B of the Ombudsman’s Notification form and, unless otherwise advised by the Ombudsman, be provided with the documentation relevant to the investigation and findings.

- Notified to the Children’s Guardian if the staff member is classified as a child related worker and there has been a finding of sexual misconduct committed against, with or in the presence of a child, or a serious physical assault of a child
• Notified to the Australian Health Practitioner Registration Agency:
  o If there is a reasonable belief of notifiable conduct by a registered health practitioner. Under the Health Practitioner Regulation National Law (NSW) notifiable conduct includes practising while intoxicated by alcohol or drugs; sexual misconduct in the practice of the profession; placing the public at risk of substantial harm because of an impairment (health issue); or placing the public at risk because of a significant departure from accepted professional standards
  o Any conduct of a registered health practitioner that the Chief Executive suspects on reasonable grounds may constitute professional misconduct or unsatisfactory professional conduct under the Health Practitioner Regulation National Law (NSW).

Service Check Register records must be created in accordance with the requirements of the NSW Health Service Check Register Policy.

Where a child related allegation, charge or conviction is work related and involves a former NSW Health staff member, the Chief Executive of the relevant NSW Health organisation must be notified, support offered to the alleged victim and reports made to external agencies as appropriate. Any available information should also be reviewed from a systemic perspective and a focus on ensuring the ongoing safety of children.

Records relating to child related allegations, charges and convictions must be kept securely and maintained for 100 years before being destroyed, noting that they may be subject to audit by the NSW Ombudsman.

IMPLEMENTATION

The following have key responsibilities in relation to this Policy Directive:

Chief Executives are required to:

• Have in place procedures for ensuring that all staff are made aware of their responsibilities for reporting child related allegations, charges or convictions involving anyone working in NSW Health

• Have in place procedures for managing child related allegations, charges or convictions, including the requirement for the Chief Executive to be notified.

Workforce Directorates / Human Resource Departments / Internal audit Units / Governance or Professional Conduct and Standards Units are required to

• Ensure provision of information, advice and monitoring as necessary to support effective implementation of this policy.

All staff are required to:

• Notify their line manager or supervisor, or other delegated position, as specified in local procedures, if they become aware of any child related allegations, charges or convictions involving a NSW Health staff member

• Self-disclose any child related criminal charges and/or convictions against them.
1 BACKGROUND

1.1 About this document

Child related allegations, charges and convictions involving anyone engaged in work in NSW Health, whether for paid or unpaid work, must be managed in accordance with this Policy Directive and Procedures and consistent with the processes outlined in the NSW Health policy on Managing Misconduct, or in the case of staff of the Ministry of Health, the Government Sector Employment Act 2013, supported by the NSW Public Service Commission’s Employment Portal. These Procedures set out the requirements for managing child related allegations, charges and convictions, where the requirements vary from, or are in addition to, those of the NSW Health policy for Managing Misconduct.

This Policy Directive and Procedures should be read in conjunction with other relevant NSW Health policies, such as those on Child Wellbeing and Child Protection, Sexual Assault Services, Service Check Register for NSW Health, Managing Concerns or Complaints About Clinicians and Incident Management.

1.2 Key definitions

Child is, for the purpose of this policy, a person under the age of 18 years of age as defined by the Ombudsman Act 1974 and the Child Protection (Working with Children) Act 2012. Refer to section 1.3.3 of these Procedures for the definition of a child and young person under the Children and Young Person’s (Care and Protection) Act 1998.

Child related allegation is an allegation or criminal charge against a current NSW Health staff member that involves reportable conduct or misconduct that may involve reportable conduct.

Child related conviction is a conviction, including a finding of guilt without the court recording a conviction, against a NSW Health staff member, for an offence involving reportable conduct.


Class of children is a group of children who may be at risk of harm from abuse because of a person or situation.

NSW Health Child Wellbeing Units are units staffed by child protection professionals who are able to provide telephone advice and support to NSW Health workers in determining the level of risk of harm and responding to the needs of vulnerable children, young people, pregnant women and families.

NSW Health organisation is, for the purposes of this policy, any public health organisation as defined under the Health Services Act 1997, NSW Ambulance, Health Infrastructure, HealthShare NSW, NSW Health Pathology, E-Health, any other administrative unit of the Health Administration Corporation, and Albury-Wodonga Health in respect of staff who are employed in the NSW Health Service, and the NSW Ministry of Health.

NSW Health Service includes all persons employed under Chapter 9, Part 1 of the Health Services Act 1997.

JIRT is a Joint Investigation Response Team made up of the Department of Family and Community Services (FACS), NSW Police Force and NSW Health Professionals working collaboratively to jointly manage statutory child protection matters (reports of sexual abuse and serious physical abuse and neglect of children and young people) that require a criminal justice and health response.
Reportable conduct is defined under Part 3A of the *Ombudsman Act 1974* as:

- Any sexual offence, or sexual misconduct, committed against, with or in the presence of a child (including a child pornography offence or an offence involving child abuse material) or
- Any assault, ill treatment or neglect of a child or
- Any behaviour that causes psychological harm to a child whether or not, in any case, with the consent of the child.

The Ombudsman Act also states that reportable conduct does not include:

- Conduct that is reasonable for the purposes of the discipline, management or care of children, having regard to the age, maturity, health or other characteristics of the children and to any relevant codes of conduct or professional standards, or
- Use of physical force that, in all the circumstances, is trivial or negligible, but only if the matter is to be investigated and the result of the investigation recorded under workplace employment procedures.

For further information about what constitutes reportable conduct, refer to the NSW Ombudsman’s Fact Sheet *Defining Reportable Conduct*.

**Staff member**, for the purpose of this policy, is anyone working in NSW Health, whether as a paid staff member or engaged in any other capacity, including as a volunteer, Visiting Practitioner, student attending clinical placement or anyone else appointed on an honorary or contractual basis.

### 1.3 Legal and Legislative Framework

#### 1.3.1 Ombudsman Act 1974 and Ombudsman Regulation 2011

The *Ombudsman Act 1974* and the *Ombudsman Regulation 2011* prescribe the responsibilities of heads of agencies for preventing, and for responding to, child related allegations, charges and convictions against staff. Consistent with this Act, NSW Health Chief Executives are required to notify the NSW Ombudsman of all child related allegations, charges or convictions involving NSW Health staff as soon as is practical or at the latest within 30 days of becoming aware of the matter.

Child related allegations and convictions notifiable to the Ombudsman include conduct that has occurred outside of work or prior to the staff member’s engagement in NSW Health, including historic matters where the alleged victim may now be an adult.

NSW Health organisations are required to inform the Ombudsman of the results of their investigations into child related allegations and convictions and the action taken, or proposed to be taken, in response to such allegations or convictions.

Chief Executives are also required to ensure that all staff are informed of their obligation to notify the Chief Executive when they become aware of any child related allegation, charge or conviction against anyone working in NSW Health, and to ensure that there are clear internal reporting lines to facilitate this.

For further information, including contact details for the NSW Ombudsman’s office, refer to the Ombudsman’s website at [www.ombo.nsw.gov.au](http://www.ombo.nsw.gov.au)
1.3.2 The Child Protection (Working with Children) Act 2012

The Child Protection (Working with Children) Act 2012 requires notifications to the Office of the Children’s Guardian (the Children’s Guardian) of investigation findings where a child-related worker has been found to have engaged in either sexual misconduct (including sexual offences) committed against, with, or in the presence of a child, or a serious physical assault of a child.

The notification should be completed as soon as a final determination has been made by the NSW Health organisation that sexual misconduct or serious physical assault has occurred, even if appropriate disciplinary action in respect of the misconduct has not yet been determined or review or appeal processes remain available.

For further information about matters requiring notification to the Children’s Guardian, refer to their Fact Sheet ‘Information for Reporting Bodies: Reporting Certain Misconduct Involving Children’.

1.3.3 Children and Young Persons (Care and Protection) Act 1998

The Children and Young Persons (Care and Protection) Act 1998 provides for the care and protection of, and the provision of services to, children and young people. Under this Act, a child is defined as a person who is under the age of 16 years and a young person is a person who is aged 16 and above but under the age of 18 years.

A key object of this Act is for all institutions, services and facilities responsible for the care and protection of children and young people to provide an environment for them that is free of violence and exploitation. It prescribes the role of the Community Services and the role of families, agencies and communities in relation to child protection, and the role of mandatory reporters. It also provides the mechanisms by which prescribed bodies may exchange information relating to the safety, welfare or well-being of a particular child or young person or class of children or young persons. For further information, refer to the current NSW Health policies on Child Wellbeing Units and Child Protection Policies and Procedures for NSW Health.

2 INITIAL REVIEW AND RESPONSE

A child related allegation or conviction may arise or be identified through a number of sources, including:

- Information provided from a Child Wellbeing Unit, JIRT Referral Unit, local JIRT Unit, the Police, Family and Community Services, to the NSW Health organisation directly or via the NSW Ministry of Health’s Workplace Relations Branch
- Complaints or concerns, including those made by patients, their carers, or anonymously and including those relating to clinical procedures
- From a presentation to an Emergency Department or other NSW Health facility
- From a manager’s or colleague’s observations
- Self-disclosure by a staff member or
- From information in circulation in the public domain, either through formal channels arising from coverage of matters under investigation (i.e. press reporting) or informal channels (social media channels etc.).

The NSW Health policy on Child Protection should be referred to for guidance on how to respond to disclosures of child wellbeing concerns or abuse.
Once action has been taken to address any immediate risks, the information should be forwarded to the Workforce Director or equivalent of the NSW Health organisation, or other position as specified in local procedures, to determine if the matter constitutes a child related allegation or conviction requiring notification to the Chief Executive and to the Ombudsman.

### 2.1 Determining if a matter constitutes a child related allegation or conviction?

A child related allegation or conviction must contain the following three elements:

- A description of alleged behaviour or details of a criminal charge or conviction that may constitute reportable conduct, and
- The allegation or conviction is against a current NSW Health staff member as defined in section 1.2 of this policy, and
- The alleged victim was under the age of 18 years at the time of the alleged behaviour or incident.

Note that child related allegations and convictions include outside work matters, historical matters and child pornography.

### 2.2 Initial Notifications

All child related allegations and convictions are required to be:

- Reported to the Child Protection Helpline if there is suspected risk of significant harm relating to a child or a class of children (refer to the NSW Health policy on Child Protection)
  - A report to the Child Protection Helpline may also include information about the person’s role in NSW Health in relation to contact with children, any risk management action planned or being taken and a contact person for consultation and ongoing exchange of information.
  - Where there are concerns about a child that do not meet the threshold for a mandatory report, the NSW Health Child Wellbeing Unit must be contacted.
- Reported to the NSW Police if there is alleged criminal conduct; this reporting requirement is in addition to any report to the Child Protection Helpline, and includes matters that may not meet the threshold for a report to the Child Protection Helpline (for example, child pornography, historical abuse, etc.).
- Notified to the relevant NSW Health Chief Executive (or Secretary, NSW Health in the case of the NSW Ministry of Health staff).
  - Where the person works in a different NSW Health organisation to where the alleged reportable conduct has been identified, information must be immediately forwarded to the relevant other NSW Health organisation to manage the allegation against the staff member. This would usually be through the relevant Workforce Director or equivalent.
  - In these cases, the NSW Health organisation that identified the allegation is still responsible for ensuring any immediate safety or child protection issues are addressed, including reporting to the Child Protection Helpline, Child Wellbeing Unit, Police, referral to Sexual Assault Services, etc.
  - Information about any immediate risk action taken should be also provided to the NSW Health organisation where the staff member works.
• Notified to the NSW Ombudsman using Part A of the Ombudsman’s Notification Form as soon as possible and in any event within 30 days of the matter being brought to the attention of the NSW Health organisation.
• Notified within 24 hours to the NSW Ministry of Health via a Reportable Incident Brief (RIB).
• If there is a reasonable belief that a registered health practitioner has behaved in a way that constitutes notifiable conduct, professional misconduct or unsatisfactory professional conduct under the Health Practitioner Regulation National Law (NSW), a notification is required to the Australian Health Practitioner Regulation Agency.

3 MANAGING RISKS

A risk assessment and ongoing risk management strategy must be put in place as soon as possible, consistent with the requirements in the NSW Health policy on Managing Misconduct, which outlines the options available for managing risk involving NSW Health employees. A Risk Assessment template is available on the NSW Health Intranet.

Where risk management action is required to be taken against the staff member, the NSW Health policy on the Service Check Register should be reviewed to determine any requirement for the creation of a Service Check Register record.

To ensure that child protection and patient safety issues and / or victim needs’ are considered and addressed, the management of child related allegations and convictions should include consultation with child protection workers, sexual assault services and / or senior clinical staff, as relevant.

3.1 Responsibilities to the alleged victim

The NSW Health organisation has a responsibility to ensure that, as far as possible, the needs of any alleged victims and their non offending family are being addressed, and appropriate crisis assessment and treatment, counselling, medical services or sexual assault services are offered, as appropriate.

The NSW Health organisation should ensure that the alleged victim and / or their non offending family are advised of the responsibilities of the NSW Health organisation in respect of child related allegations and convictions and that they are provided with information about the progress of any investigation, advised of the findings and are kept informed of any action planned or being taken in response to the alleged conduct.

They should also be advised of NSW Health’s reporting requirements to the NSW Ombudsman, the NSW Police and to Family and Community Services, as applicable and offered support in making a report to the NSW Police themselves, as appropriate. A nominated NSW Health contact should also be made available to them during the process.

The NSW Health organisation should liaise with the relevant contact officer of the NSW Police, JIRT or Community Services if they are involved in the matter, regarding the needs of the alleged victim and / or their non offending family.

3.2 Advising the staff member

The timing of advice to a staff member about a child related allegation should be part of the risk assessment and should involve consideration of the following factors:

• Does the information received require further clarification before it can be determined if it meets the threshold for reportable conduct?
• Are there any particular risks that would suggest the timing of the advice needs to be delayed (for example, a statement is yet to be obtained from an alleged victim)?
• Is immediate risk management action required necessitating advice to the staff member?
• Has an external agency, such as the Police or Family and Community Services, asked the NSW Health organisation to delay notifying the staff member?

• Has a notification been made to the Child Protection Helpline or the NSW Police, and if not, does this need to be completed before any advice is provided to the staff member?

• In all circumstances, the paramount responsibility of the NSW Health organisation is the protection of all children in its care; where there are identified risks requiring risk management action, this should be conveyed to the external agency, along with a timeframe for commencing the risk management action and the associated advice proposed to be provided to the staff member.

Any decision to delay notifying the staff member should be clearly documented.

The staff member should be advised of the responsibilities of the NSW Health organisation in responding to child related allegations and convictions, provided with information about the process, offered support as required and afforded procedural fairness. Refer to the Managing Misconduct policy for further information.

They should also be advised, at an appropriate time, of the notification requirements to the Ombudsman’s Office and at the conclusion of the investigation, be provided with details of any findings with regards to reportable conduct and any requirement to notify the Office of the Children’s Guardian.

4 INVESTIGATION

Irrespective of any action the Police or any other external agency may take, NSW Health organisations are required to investigate (unless the facts are clear and uncontested, such as with convictions) child related allegations and to make their own findings and decisions about any disciplinary action.

The NSW Health organisation should generally not commence an internal investigation until they have been given the clearance to do so by the external agency or until the external agency has completed their inquiries, and all child protection / criminal investigations have concluded or been closed. Consultation with any external agencies must take place to ensure that any external investigations are not compromised.

4.1 Concurrent Community Services, Police or JIRT investigation

Where NSW Police / JIRT / Family and Community Services are undertaking a criminal / child protection investigation, or have advised that they may undertake such an investigation, an ongoing liaison should be maintained to ensure that criminal, child protection and disciplinary investigations are coordinated effectively, and that information is exchanged as required to assist in the ongoing assessment and management of risk.

The NSW Health organisation must still complete all relevant notifications and continually assess and manage the risks based on available information but would generally not commence its internal investigation until the external investigations and any associated proceedings have concluded and the external agency has indicated that they have no objections to NSW Health commencing its investigation.

The NSW Health organisation should request information from any external agencies involved in the matter to assist in assessing potential workplace risk and to assist in completing its investigation, when appropriate to do so. In certain circumstances it may be necessary to clarify with the Police whether they have closed or suspended their investigation and the extent of the information that may be provided to the staff member.
Information requested may include details of the complaint or disclosure (including the name and age of the alleged victim if not already known), records of interview with the alleged victim or any other relevant parties and any other relevant information. A template letter is available on the NSW Health Intranet.

The NSW Health organisation must:

- Review the information provided by the external agency
- Identify and undertake any further enquiries or information as required
- Determine what needs to be put to the staff member for response, and
- Make its own findings.

Where the matter has been before the courts, information may also need to be requested about the court outcome; this should be done by asking the staff member to provide relevant documentation. It may also be appropriate to write to the court to request information. A template letter is available on the NSW Health Intranet.

In limited circumstances, if the NSW Health organisation is satisfied, after reviewing the information provided by the external agency, that it conclusively demonstrates that the allegation was false and that no further information is required, the matter may move directly to a finding and the staff member advised.

Where an external agency has substantiated an allegation, but there is no criminal conviction, the NSW Health organisation must still afford the staff member procedural fairness and make its own findings.

In exceptional circumstances, it may be appropriate to commence and conclude the employer investigation while the external criminal or child protection investigations are ongoing, noting that the Ombudsman’s office may still request that the NSW Health organisation monitor the outcome of the external proceedings. However, there must be close and ongoing liaison with the Police and / or Family and Community Services, as well as ongoing consideration and management of the risks associated with this course of action; these risks include the contamination of a criminal investigation as well as unnecessary interviewing of victims, not having access to all relevant evidence and management of a staff member’s right to silence in criminal matters, etc.

The reason for commencing the investigation in these circumstances must be documented and approved by the Chief Executive or their delegate.

### 4.2 Managing Child Related Criminal Charges

For child related criminal charges, it is generally appropriate to wait until the court process has been completed before finalising the employer investigation. All relevant notifications should still be made and a risk assessment completed.

To assist in the risk management decision making, the staff member should be asked for information and any relevant documentation regarding:

- The charges against them
- Any statements they have provided to the police
- Court dates
- How they intend to plead and
- Any other information that may be relevant to assess the risks.
Information should also be requested directly from the Police, Family and Community Services and / or courts.

Should the matter not proceed to a conviction or finding of guilt, the matter should be dealt with as an allegation and the NSW Health organisation must complete its investigation and make its own findings.

Should the court proceedings result in a conviction or a finding of guilt, the NSW Health organisation should obtain details of the conviction or finding of guilt, complete its risk assessment to determine whether any action is required to be taken against the staff member, provide the staff member with procedural fairness regarding any proposed adverse action and finalise the matter in accordance with the requirements of this policy and consistent with the Managing Misconduct policy.

In certain limited circumstances it may be appropriate to finalise the investigation in terms of making findings and decisions about disciplinary action, subject to procedural fairness requirements as above, prior to the completion of the court process, for example, where a guilty plea has been entered, noting that the Ombudsman’s office may still request that the NSW Health organisation monitor the outcome of the external proceedings.

4.3 Interviewing children

For child related allegations, consideration must always be given to whether it is necessary to interview the child who is the alleged victim.

In certain situations, it may not be appropriate or necessary to interview the child. Where this decision is made, it must be clearly documented and included in the final investigation report. Factors that may affect the decision to interview the child include:

- Sufficiency of the available information about the alleged conduct, i.e. for a young child, it has been reported by a colleague / parent who directly witnessed the alleged behaviour and they have provided detailed information

- The child has already been interviewed by an external agency and the NSW Health organisation has obtained details of the interview:
  - If there are concerns about the sufficiency of the information obtained, they should be raised with the external agency.

- The child’s age / developmental stage or other factors impact on the child’s ability to provide detailed information.

- Whether the child parents / guardians consent to their child being interviewed and for older children whether the child also consents

- Any other factors that indicate an interview may result in further trauma or be detrimental to the welfare of the child.

A decision to interview a child must be made in consultation with child protection workers, and if a child is to be interviewed, it must only be by persons with sufficient skill or expertise in obtaining children’s evidence. Child protection staff and in some instances Aboriginal Health workers may be best placed to conduct an interview with a child.
5 ISSUES ARISING IN CHILD RELATED MATTERS

5.1 Allegations arising from clinical procedures

Where a child related allegation has arisen out of a clinical procedure, it must still be managed in accordance with this policy; however the NSW Health policy on Managing Complaints or Concerns about Clinicians should also be consulted.

In certain cases, to assist in the initial review in determining whether the allegation meets the definition of reportable conduct (see section 1.2), an appropriately qualified and independent clinician may need to review whether the conduct being alleged is reasonable for the purpose of the management or care of the child having regard to their age, maturity, health or other characteristics and to any relevant code of conduct or professional standard and therefore whether further investigation under this policy is warranted.

A decision that the allegation or complaint does not constitute an allegation of reportable conduct and therefore is not required to be managed as a child related allegation under this policy should be approved by an appropriately delegated person and the records maintained securely and centrally, noting that such records may be subject to audit by the NSW Ombudsman.

5.2 Anonymous allegations

Anonymous allegations must still be managed in accordance with this policy.

Action taken will depend on the level of detail provided, and the ability to obtain further detail. Where there is insufficient information or details to make any enquiries or take any action, this should be noted and the complaint filed in a secure and confidential place.

Where the information provided meets the definition of alleged reportable conduct, an Ombudsman notification is required and the NSW Health organisation is required to complete an investigation, make findings and decisions about any disciplinary action.

When assessing action to take in response to an anonymous complaint, the following factors should be considered:

- Any details in the allegation that can be confirmed or refuted (for example, was any context provided, were there details of the alleged behaviour, was there a time frame, was any workplace named or details of any alleged victims or witnesses or any physical or other evidence provided)
- Contact with the NSW Police and FACS to confirm if they have any information in relation to the allegation; and if so that they give their consent to that information being put to the staff member
- Is the complainant able to be identified and contacted if further clarification is required? Note that non identification of the complainant does not preclude action being taken

5.3 Non work related and historical child related allegations

Non work related and historical child related allegations, charges or convictions against current NSW Health staff, including matters where the alleged victim is now an adult, must still be managed in accordance with the requirements of this policy, including:

- Reporting to the Child Protection Helpline where there is a current risk of significant harm to a child or class of children. The Online Mandatory Reporter Guide or the NSW Health Child Wellbeing Units can assist identify in determining whether the risks meet the threshold for reporting to the Helpline. If they do not meet the threshold, a referral may still need to be made to the Child Wellbeing Unit.
• Reporting to the NSW Police where there is alleged criminal behaviour.
• Offering support to the alleged victim (or their family) in making a report to the NSW Police.
• Completing an investigation (unless the facts are clear and uncontested) and making findings and managing risk.
• Completion of all other notifications in accordance with the requirements of this policy, including to the NSW Ombudsman.

5.4 What happens if the Police do not charge the NSW Health staff member or the Court makes a finding of ‘not guilty’?

For child related allegations where Police involvement has not resulted in criminal charges or in a guilty finding at court, the NSW Health organisation must still manage workplace risks while any criminal proceedings are ongoing; once they are finalised, undertake its own investigation (unless the facts are clear and uncontested), and make its own findings and complete all relevant notifications.

The NSW Health organisation’s actions should include a review of information obtained from the Police or from the court (refer to section 4); the evidence considered and the rationale for decisions made, noting there are many reasons that matters do not proceed to charges or to a conviction, where the standard of proof required is 'beyond reasonable doubt', whereas in civil matters, the standard is the 'balance of probabilities', subject to the “Briginshaw v Briginshaw principle”; that is, the more serious the potential misconduct, and therefore the more serious the consequences for the staff member, the stronger the evidence must be to support an adverse finding.

The staff member should still be afforded procedural fairness and provided with an opportunity to respond to the allegations and any proposed adverse findings or action.

5.5 Exchanging information with Family and Community Services / Police / JIRT

Where Family and Community Services / Police or JIRT have involvement in a matter or may have information relevant to the NSW Health organisation’s investigation and assessment of potential risk to the workplace, separate requests for information should be made to each external agency in accordance with Chapter 16A of the Children and Young Persons (Care and Protection) Act. A Template letter is available on the NSW Health Intranet.

Information may also need to be provided by the NSW Health organisation to Family and Community Services / Police or JIRT regarding risk management action it is taking or planning to take in response to the child related allegation and the nature of any potential risks in terms of the person’s role within the workplace.

For further information about exchanging information under Chapter 16A, refer to the NSW Health policy on Child Protection.

5.6 Allegations involving child pornography or child abuse material

Where an allegation involves child pornography or child abuse material, the NSW Police must be contacted immediately and advice sought before initiating an internal investigation or alerting the staff member. If the alleged use involves a NSW Health device, it should be quarantined without warning so that there is no opportunity for files to be deleted or the computer to be switched off or on or other evidence tampered with.

57(30/6/16)
Special care must be taken to ensure that any alleged child abuse material is not unnecessarily transmitted or disseminated within the NSW Health organisation, that it is contained and that only a limited number of nominated senior staff members are involved in any investigation and that the process for making any decisions or assessment of the material is clearly documented as part of the investigation.

As part of the response to an allegation involving child abuse material, the NSW Health organisation should audit the staff member’s use of NSW Health devices, subject to identifying any potential risks to the investigation.

The NSW Health organisation should be guided by the Police in respect of the classification of material as child pornography.

5.7 What happens if the staff member no longer works in NSW Health?

Where an allegation relates to conduct that has occurred within NSW Health by a former staff member who is not engaged in the NSW Health Service or in the NSW Ministry of Health at the time of receipt of the information, the relevant Chief Executive (or Secretary in the case of a matter relating to a person formerly engaged in the NSW Ministry of Health) must still be notified and appropriate reports to external agencies must be completed, including to the Child Protection Helpline if there is a risk of significant harm to a child or class of children, the Australian Health Practitioner Regulation Agency if the person is a registered health practitioner and the information received suggests such a notification is required, or the NSW Police if required.

The alleged victim should be offered support, as appropriate, which may include supporting them in reporting the matter to the NSW Police or to any other external oversight or investigative agency. Depending on the level of information available, the circumstances of the alleged conduct should be reviewed with a focus on ensuring the ongoing safety of children.

Refer to the NSW Health policy on Child Protection for further advice.

5.8 What if the alleged victim is now an adult?

If the allegation relates to a current NSW Health staff member, it must be managed in accordance with the requirements of this policy, regardless of the current age of the alleged victim (see section 5.3).

Refer to the NSW Health policies on Child Protection and Sexual Assault Services for further information on managing disclosures from adults.

5.9 What happens if the allegation is retracted, the complaint withdrawn, or the alleged victim wants no action taken?

In these circumstances, the NSW Health organisation is still required to fulfil the requirements of this policy, including notifying the Ombudsman, notifying Family and Community Services or the NSW Police, as warranted, providing the staff member with procedural fairness and making findings based on the available information.

Where an allegation has been retracted, a complaint withdrawn, or an alleged victim wants no action taken, whether or not another agency remains involved, the NSW Health organisation is required to seek information to understand the reasons for the retraction and consider this in the assessment of risk and evidence when making a finding.

Where the reasons relate to concerns around personal safety, the NSW Health organisation should explore with the person the different options for addressing those concerns, including the involvement of the NSW Police.
6 MAKING FINDINGS

6.1 Findings for the Ombudsman

For the purpose of the Ombudsman’s scheme, the following findings should be considered:

- **Substantiated** (i.e. a finding that the conduct occurred and is reportable conduct);
- **Not substantiated – insufficient evidence** (i.e. there is some evidence of weight however there is insufficient evidence available to reasonably establish that the alleged conduct did occur);
- **Not substantiated – lack of evidence of weight** (i.e. where the evidence is of such poor probative value or lacking in weight, such as to warrant a finding that, on the balance of probabilities, the conduct did not occur);
- **False** (i.e. where inquiries into the matter show reportable conduct or an act of violence did not occur).
  - Some of these matters may also be vexatious, for example where inquiries into the matter show the allegation was made without substance and to cause distress to the person against whom the allegation was made;
- **Not reportable conduct** (i.e. where inquiries into the matter show the conduct was not reportable).
  - For example; use of force that was trivial or negligible in the circumstances, conduct that was reasonable in the circumstances or found to be accidental. This may include ‘misconceived’ matters, where inquiries into the matter show that, even though the allegation was made in good faith, it was based on a misunderstanding of what actually occurred and the incident was not reportable conduct.

For further information, refer to the NSW Ombudsman’s Fact Sheet on making findings for child related matters.

6.2 Misconduct findings

In addition, the NSW Health organisation must make findings about whether any substantiated conduct constitutes misconduct and therefore whether remedial, disciplinary or other action (in the case of volunteers etc.) is required, consistent with the Managing Misconduct policy.

7 FINALISING THE PROCESS

7.1 Notifying affected parties of the outcome

The alleged victim and / or their family should be notified of any findings made by the NSW Health organisation and any action taken, including against the staff member in response to those findings and of any notifications made to external agencies.

7.2 Notifying the Australian Health Practitioner Regulation Agency

Where the staff member is a registered health practitioner, consideration must be given to any requirements to notify the Australian Health Practitioner Regulation Agency if such notification has not been completed already and there is a reasonable belief that the practitioner has behaved in a way that constitutes notifiable conduct, professional misconduct or unsatisfactory professional conduct under the Health Practitioner Regulation National Law (NSW).
Notifiable conduct is defined under the *Health Practitioner Regulation National Law (NSW)* as including:

- Practising while intoxicated by alcohol or drugs
- Sexual misconduct in the practice of the profession
- Placing the public at risk of substantial harm because of an impairment (health issue) or
- Placing the public at risk because of a significant departure from accepted professional standards.

Professional misconduct and unsatisfactory professional conduct are defined in sections 139B–139D of the *Health Practitioner Regulation National Law (NSW)*.

### 7.3 Notifying the Children’s Guardian

Any findings of sexual misconduct or serious physical assault against a child involving a child-related worker must be notified to the Children’s Guardian.

This must be done using the pre-existing “Working with Children Check Employer log in” details for the NSW Health organisation.

In certain circumstances, NSW Health may also provide information to the Children’s Guardian under Chapter 16A of the *Children and Young Person’s (Care and Protection) Act* if that information is considered relevant to an assessment of risk that the staff member may pose of a child or class of children.

Refer to the NSW Health policies on *Child Protection*.

For further information about requirements for notifying the Children’s Guardian and how to make a notification, refer to their Fact Sheet “Information for reporting bodies: Reporting certain misconduct involving children” available on their website.

### 7.4 Final notification to the Ombudsman

Once the investigation or other action is finalised, and findings (including those related to convictions) and final decisions made, the Ombudsman’s office must be notified using Part B of the Ombudsman Notification Form available from its website.

Unless the Ombudsman has advised otherwise, the notification should be accompanied by copies of all material relevant to the investigation and decision making, including records of interview, memorandums or in-briefs, emails, file notes of conversations and correspondence related to the matter.

The Summary of Notifications Information Sheet available on the NSW Intranet also provides further guidance on other notification considerations.

### 7.5 Service Check Register

Service Check Register records must be created in accordance with the requirement so the NSW Health policy on the Service Check Register.

### 7.6 Other action required

As part of finalising child related matters, NSW Health organisations should always review the circumstances of the alleged or substantiated conduct from a systemic perspective with a focus on ensuring the ongoing safety of children.
8 KEEPING RECORDS

Records relating to child related allegations and convictions, including false, malicious or disproven allegations should be kept on a file that is separate to the staff member’s personnel file in a central secure location, and must be retained for a minimum of 100 years and then destroyed in accordance with the State Records guidance GA 28.

Related files should be cross-linked to each other, for the purposes of future management.

All records relating to child related allegations and convictions, including where a decision has been made that a matter is not reportable to the Ombudsman, may be audited by the NSW Ombudsman’s Office.

Records relating to the management of child related allegations are subject to the provisions of the Government Information (Public Access) Act 2009.

PHOTO AND VIDEO IMAGING IN CASES OF SUSPECTED CHILD SEXUAL ABUSE, PHYSICAL ABUSE AND NEGLECT (PD2015_047)

PURPOSE

The purpose of this Policy Directive is to:

- Define the NSW Health requirements and minimum standards for the use and management of photo and video imaging in cases of suspected child sexual abuse, physical abuse and neglect
- Guide NSW Health staff when capturing, storing and managing images for the purpose of documenting health and clinical features and informing possible future judicial proceedings that require medical opinion.

MANDATORY REQUIREMENTS

This policy requires that:

- The immediate and longer-term physical and emotional needs of the child and their parent(s) / guardian(s) are identified and taken into account when considering photo and video imaging.
- Imaging is captured for the primary purpose of documenting a clinical finding for the health care record and limited other relevant purposes, and is not excessive or unreasonably intrusive.
- Imaging is only captured where informed consent is sought and obtained for each purpose for which it may be used.
- Capture, recording and storage of images is limited to LHD / SCHN owned memory devices.
- Images are stored securely and are stored separately from the principal health care record, to maintain patient privacy.
- Limited access is provided to images, to maintain patient privacy.
- Capture, use and management of photo and video images in cases of suspected child abuse is conducted in accordance this Policy Directive, in conjunction with:
  Child Wellbeing and Child protection Policies and Procedures for NSW Health (PD_2013_007)
  Current Standards and Practice Guidelines for NSW Health Sexual Assault Services

IMPLEMENTATION

Chief Executives are responsible and accountable for:
• Establishing mechanisms to ensure the directives and requirements of this policy are applied, achieved and sustained
• Ensuring that NSW Health staff understand and are aware of their obligations in relation to this policy and related policies and procedures
• Ensuring resources are available to deliver and meet the directives and requirements of this policy
• Ensuring that NSW Health staff are trained to operationalise and implement this Policy
• Ensuring NSW Health staff are advised that compliance with this policy is part of their patient / client care responsibilities
• Ensuring that procedures for capture, storage, access and security are subject to risk analysis reassessment over time.

Facility managers are responsible for:
• Ensuring the requirements of this policy directive are disseminated and implemented in their service / department / hospital
• Establishing local validated processes for image preparation, capture, processing, storage, transmission, archiving, retention and disposal
• Monitoring implementation and compliance with this policy.

NSW Health workers are responsible for:
• Implementing and complying with the directives and requirements of this policy
• Ensuring that their knowledge of consent, privacy and documentation management processes is maintained, consistent with the requirements of this policy directive.

1 INTRODUCTION

1.1 Rationale

Clinical evaluation of a child or young person who is suspected of having been abused or neglected involves a holistic assessment of their physical needs, psychosocial needs, medical history, and any social or familial risk factors. NSW Health practitioners are required to document and report suspicion of harm and may use clinical photo and video imaging to supplement and enhance the detail in written notes and diagrams. Imaging can assist the physician to review the facts associated with clinical examination and history as part of their clinical diagnosis: in an attempt to ensure the accuracy of a diagnosis this may include professional peer review. Diagnoses in cases of suspected child abuse have an impact on the safety, welfare and wellbeing of a child or young person. Clinical photo and video imaging is an important tool in the achievement of accurate clinical conclusions to support the needs of children and young people.
This policy defines the NSW Health requirements and minimum standards for the use and management of photo and video imaging in cases of suspected child sexual abuse, physical abuse and neglect. It will guide NSW Health workers to know what actions to take when capturing, storing and managing images for the purpose of documenting health and clinical features, and informing possible future judicial proceedings that require medical opinion. A development group was convened to inform the development of this policy. Details of membership appear at Appendix 5.5.

1.2 Who this policy applies to

This policy applies to NSW Health workers in Local Health Districts (LHDs) and the Sydney Children’s Hospitals Network (SCHN) who are employed or contracted to capture or manage imaging in cases of suspected child abuse, including:

- Medical practitioners or other specialist staff undertaking medical and forensic examinations of children and young people aged under 18 who are suspected of having been sexually abused, physically abused or neglected
- Psychosocial, sexual assault and child protection practitioners, coordinators and managers
- Medical photographers, Joint Investigation Response Teams (JIRTs), Aboriginal health services and other clinical and allied health staff
- Managers or officers who support the capture, viewing, accessibility, transmission or management of photo and video imaging. This includes data custodians, IT technical and support staff, health information managers and staff in medical records departments.

The policy may also be of interest to:

- NSW Health interagency child protection partners
- Those who work in the wider criminal justice setting and child health and advocacy settings
- Networks that support children and young people who have experienced sexual abuse, physical abuse or neglect and their non-offending family members
- Those who work in private health settings who wish to adopt minimum standards for the use and management of photo and video imaging in cases of suspected child abuse.

1.2.1 Exclusions

This policy does not apply to:

- Sexual abuse examinations utilising clinical colposcopic equipment without capture of imaging
- Photo and video imaging taken in other types of medical examinations (i.e. those that do not relate to suspected child abuse)
- Medical imaging such as Magnetic Resonance Images (MRIs), Computerised Tomography (CT) scans, skeletal surveys, radioisotope scans or post-mortem imaging.

1.3 Service users

Children or young people who use NSW Health services in relation to suspected sexual abuse, physical abuse and/or neglect and, depending on the age of a young person, this may include parent(s), carer(s) or guardian(s).
1.4  Context for practice

1.4.1  Interagency context

Medical and forensic examinations and associated photo and video imaging take place in the context of an interagency response to child protection. Interagency roles and responsibilities are outlined in the Child Wellbeing and Child Protection Policies and Procedures for NSW Health, 2013, current standards and guidelines for NSW Health Sexual Assault Services and NSW Interagency Guidelines.

1.4.2  NSW Health context

The psychosocial and medical needs of a child or young person are a priority and need to be responded to appropriately. NSW Health’s role is to provide an integrated psychosocial and medical response to all suspected child abuse presentations including assessment, crisis intervention and counselling. The medical response will potentially include a medical and forensic examination. Medical and forensic examinations are critical to the crisis response required on presentation of: a child victim of sexual abuse to a Sexual Assault Service or Emergency Department; or a child with suspected physical abuse or neglect to a medical practitioner, Emergency Department, or other health service.

Related child protection and violence prevention, privacy, security and document management policies are listed in Appendices 5.1 to 5.4.

1.4.3  Clinical context

Clinical photography has assisted in the development of medical knowledge and skills within the NSW Health workforce over the last two decades, and aided the interpretation and evaluation of injuries, for the benefit of examiners and their patients. Medical and forensic assessment of children suspected of having been abused occurs within a framework that responds to the immediate psychosocial and medical needs of a child and their family – who are often traumatised and distressed.

This context includes:

- Identification of children at risk who require a medical and forensic assessment
- Recording of medical history and examination findings complemented by appropriate clinical photo or video imaging
- Forensic specimen collection where relevant (as in recent sexual abuse)
- Medical treatment of injuries or other sequelae of the abuse, such as the risk of exposure to sexually transmitted diseases or pregnancy
- Interpretation of clinical findings, with a reference to any allegation of abuse.

Anatomical diagrams are useful for recording certain features of an injury, such as the number of injuries, the type of injuries, their overall size and shape and the general location of the injuries on the body. It is difficult for a doctor to record adequately sufficient information for detailed medical and forensic assessment of many injuries with diagrams and words alone. Medical illustration is a specialised career. It takes both skill and time to produce an accurate and useful medical drawing. The extra detail provided by a photo or video record is of particular relevance when a medical and forensic examiner is asked to comment, sometime after the medical examination, on whether a particular account of accidental injury, provided by a caregiver, might reasonably account for the clinical findings.

56(29/10/15)
Several advantages of photography can be summarised as below:

- Photo and video images allow review of injuries or other clinical findings, such as evidence of dermatological conditions or malnutrition, in a more comprehensive manner. Indeed there are many reasons why a child’s injuries may need to be reviewed. The original examining doctor may review photos when preparing an expert certificate and/or prior to appearing in court. Photo and video imaging can assist the examining doctor when they review the patient for ongoing clinical care, or if the police provide additional information and ask for a clinical opinion, in regards injury causation. Photo and video imaging is useful for gaining a second opinion by a senior colleague as to the significance of the injury and also helps determine if specialist referral is necessary. It may also prevent the need for a child to travel long distances to a specialist centre.

- Imaging can overcome the difficulties presented by children and young people having to lie still for extended periods of time. Children can naturally wriggle and not want to lie still – especially if they have experienced sexual abuse or if there is injury or recent assault. This is particularly relevant to examining the ano-genital regions, especially in pre-pubertal females where there is a need to assess in detail the significance of small anatomical structures which may be a normal variant or an indicator of recent or earlier injury.

- Sexual abuse assessment in pre-pubertal children is complex. Paediatric genital anatomy is variable and accurate observation and interpretation is difficult. Forensic colposcopic imaging allows the examination to proceed with the knowledge that a child or young person can benefit from subsequent specialist review of the imaging as a record of the complex clinical findings.

- Photo and video imaging may enable the medical examiner to capture a clear picture of an area that was only exposed for a few seconds. The use of photo and video imaging can in many cases prevent the need for a child or young person to return for a repeat examination, or undergo examination under anaesthesia.

It is best practice in Forensic Medicine to rigorously separate the observation and recording of findings from the interpretation of those findings. Photo and video imaging enables the examiner to concentrate on observation, which is demanding, and then to later consider all possible causes.

1.4.4 Intimate images, sensitive evidence and retention

Photo and video imaging captured as part of a medical and/or forensic assessment may include intimate images.

Intimate images are defined as depicting the genitalia, anus or post-pubertal female breast (Faculty of Forensic & Legal Medicine, 2014) and may also include other parts of the body, such as the buttocks or chest of a pre-pubertal child.

These images are considered as 'sensitive evidence' under the Criminal Procedure Act 1986 (Section 281B). Where they are held by the NSW Police Force and Office of the Director of Public Prosecutions (ODPP) access to them is restricted. These restrictions do not extend to images held by NSW Health. Where a subpoena has been validly lodged, the court is not obliged to restrict access to intimate images held by NSW Health.

In accordance with health care record retention policies, once an image is captured as a medical record it can be subpoenaed, shown in court and remains on a medical record file for at least 30 years (NSW Government General Retention and Disposal Authority policy, 2004, revised 2011).
# 2 NSW Health Minimum Standards

When use of photo and video imaging is being considered during medical and forensic examinations in cases of suspected child sexual abuse, physical abuse and neglect, NSW Health will ensure that:

<table>
<thead>
<tr>
<th>1.</th>
<th>The immediate and longer-term physical and emotional needs of the child and their parent(s)/guardian(s) are identified and taken into account. (Section 2.1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Imaging is captured for the primary purpose of documenting a clinical finding for the health care record and other directly related purposes, and is not excessive or unreasonably intrusive. (Section 2.2)</td>
</tr>
<tr>
<td>3.</td>
<td>Imaging is only captured where informed consent is sought and obtained for the specific purposes for which it may be used. (Section 2.3)</td>
</tr>
<tr>
<td>4.</td>
<td>There are standardised procedures for capturing and documenting images to reduce variation across statewide services. (Section 2.4)</td>
</tr>
<tr>
<td>5.</td>
<td>Capture, recording and storage of images is limited to LHD/SCHN owned memory devices. (Section 2.5)</td>
</tr>
<tr>
<td>6.</td>
<td>Images are stored securely and separately from the principal health care record, to maintain patient privacy. (Section 2.6)</td>
</tr>
<tr>
<td>7.</td>
<td>Restricted access is provided to images, to maintain patient privacy. (Section 2.7)</td>
</tr>
<tr>
<td>8.</td>
<td>The integrity of images is maintained in the longer-term. (Section 2.8)</td>
</tr>
</tbody>
</table>

## 2.1 Physical and emotional needs of the child or young person

**Standard:** The immediate and longer-term physical and emotional needs of the child and their parent(s)/guardian(s) are identified and taken into account when considering photo and video imaging.


- In cases of suspected physical abuse and neglect, optimally, assessment should be conducted by the medical officer with a social worker or other health professional colleague, e.g. a nurse, present to facilitate a holistic assessment ([Suspected Child Abuse and Neglect (SCAN) Medical Protocol, 2014](http://www.health.nsw.gov.au/healthtopics可愛 violence/documents/Critical incidents and concerns for child health staff.pdf)).


When deciding whether and how to capture images in this context, NSW Health workers must:

- Identify and take into account:
  - Factors arising from the life circumstances of the child or young person, their psychosocial development, vulnerability to particular risks and their linguistic, cultural and religious needs
  - The circumstances in which the child or young person was alleged to have been assaulted, abused or neglected
− The need for an appreciation and understanding of Aboriginal people and communities’ inter-generational trauma legacies, the impact of power dynamics, the importance for understanding an Indigenous world-view, including cultural practices and protocols, the multiple and inter-related factors that contribute to the poorer health status of Aboriginal people, and the limitations of Western approaches in the assessment and treatment of trauma (see http://www.health.nsw.gov.au/aboriginal/pages/default.aspx).

• Ensure that children, young people and their parent(s)/guardian(s) have:
  − Access to health information relative to their wellbeing
  − The opportunity to participate in decision making
  − Access to an interpreter if required (see Interpreters – Standard procedures for working with Health Care Interpreters)
  − Access to an Aboriginal Health worker if desired. It is important to determine at the beginning the most appropriate person or people to communicate with in relation to the patient.

2.2 Purpose of imaging

Standard: Imaging is captured for the primary purpose of documenting a clinical finding for the health care record and other directly related purposes, and is not excessive or unreasonably intrusive

In accordance with the NSW Health Privacy Manual for Health Information, 2015:

• The primary purpose for collecting photo and video imaging is to document a clinical finding for the medical record
• Imaging must be relevant to the purpose, not excessive, accurate, up to date, complete and must not be unreasonably intrusive
• Collection of photo and video imaging must supplement, not replace, other methods of documenting findings
• Other directly related purposes for collecting photo and video imaging may include:
  − Peer review to assist diagnosis
  − Providing an aide-memoire for potential future legal proceedings
  − Teaching, research and quality improvement activities (sections 2.3.3, 2.7.1, 2.8 and 2.9).

LHDs/SCHN must ensure that images are only captured and used for relevant purposes in accordance with the NSW Health Privacy Manual for Health Information, 2015.

2.3 Seeking consent

Standard: Imaging is only captured where informed consent is sought and obtained for the specific purposes for which it may be used

LHDs/SCHN must ensure that NSW Health workers act in accordance with the NSW Health Consent to Medical Treatment - Patient Information policy, 2005 and the NSW Health Privacy Manual for Health Information, 2015 and comply with 2.3.1 to 2.3.3 below. Additional advice may be sought from NSW Health Legal and Regulatory Services.
2.3.1 Who should seek consent

An examiner must ensure that valid consent has been obtained. An examiner may ask another health care practitioner to seek consent, however the examiner maintains responsibility and may be held responsible in some circumstances if consent is not sought correctly (NSW Health Privacy Manual for Health Information, 2015).

2.3.2 Who can provide consent

Where a child or young person is less than 14 years of age, consent given by a parent or legal guardian is generally necessary. In some circumstances, consent can be given by the young person if he or she is considered by the treating health care practitioner to be mature enough, and if this would be appropriate in the circumstances. See 'Gillick competence' in the 'Glossary'.

Where a young person is aged 14 or 15 they are generally able to consent, however an assessment of their maturity and understanding will still need to be made. Effort should be made to seek the consent of a parent or legal guardian unless the young person indicates a strong objection, and this is reasonable in the circumstances. Alternatively a parent or legal guardian can provide consent, however it would be exceptional to proceed on the basis of parent or guardian consent without the acquiescence of the young person aged 14 or 15.

Where the young person is 16 years of age or over they should generally be capable of consenting themselves (NSW Health Consent to Medical Treatment - Patient Information policy, 2005; NSW Heath Privacy Manual for Health Information, 2015).

For guidance on capacity to consent see the NSW Health Consent to Medical Treatment - Patient Information policy, 2005 and the NSW Heath Privacy Manual for Health Information, 2015.

Occasionally, a parent delegates their responsibility for consenting to medical treatment on behalf of their minor child, to another adult. This may occur in certain cultures, for example, in relation to Aboriginal children, where an extended family member, rather than the child’s mother or father, might be responsible for giving consent on their behalf. Where NSW Health workers require advice about who is able to provide consent for imaging they should consider the following options:

- Refer to policy relating to:
  - The broader context of consent for the examination (NSW Health Consent to Medical Treatment - Patient Information policy, 2005; NSW Heath Privacy Manual for Health Information, 2015)
  - Child Wellbeing and Child protection Policies and Procedures for NSW Health, 2013 and current standards and guidelines for NSW Health Sexual Assault Services
- Contact NSW Health Legal and Regulatory Branch or NSW Kids and Families during business hours
- Contact the Guardianship Division of the NSW Civil and Administrative Tribunal.

2.3.3 The consent process

Where child sexual abuse, physical abuse or neglect is suspected and the capture and use of photo and video imaging is considered as part of a medical and forensic examination, informed consent must:

- Be sought in accordance with the NSW Health Consent to Medical Treatment - Patient Information policy, 2005 and the NSW Health Privacy Manual for Health Information, 2015 and
- Address consent for the capture of the image(s) and the separate specific purposes for which image(s) may be used.
The consent process must include:

- Patient/parent/guardian access to culturally appropriate information
- Seeking written informed consent for the capture of photos to document a clinical finding
- An explanation to the child or young person and/or their parent(s)/guardian(s)
  - What the procedure for capturing imaging will involve
  - That imaging may include ano-genital and breast/chest areas of the body and that they may opt to exclude imaging of these or other specific body areas
  - That any records of examinations, findings, photos, videos, samples/specimens taken in accordance with the consent/s given
    - Will be stored in accordance with NSW Health: Health Care Records – Documentation and Management policy, 2012 and the NSW Government General Retention and Disposal Authority policy, 2004 (revised 2011) for a minimum of 30 years
    - May be referred to another clinician for a second opinion and peer review
    - May be forwarded to the NSW Police Force, ODPP, and by the court under subpoena, including the judge, the jury, the defendant, counsel for both prosecution and defence and any other people whom the judge considers relevant
    - May be produced to comply with a request to a NSW Health organisation under the legislation set out in the Children and Young Persons (Care and Protection) Act 1998
    - May be forwarded to parties in Family Court proceedings under subpoena

For the purpose of this policy the consent process must also include:

- Seeking separate informed consent for the use of copies of photo and video imaging for a) teaching and/or b) approved research. All such copies must be de-identified, the teaching and research activities must be compliant with the NSW Health Privacy Manual for Health Information, 2015 and other relevant NSW Health policies and research must be approved by a Research Ethics Committee (for example, see https://hrep.nhmrc.gov.au/certification/hrecs, http://www.ahmrc.org.au/ethics2.php and www.ipc.nsw.gov.au/statutory-guidelines-research-purposes-pdf). Human Research Ethics Committees – Quality Improvement & Ethical Review: A Practice Guide for NSW can help to determine whether an activity constitutes a research or quality improvement activity.
- An explanation that consent for the future use of images for a) teaching and/or b) approved research activities may be withdrawn by the person who provided consent or the person depicted in the image(s) once they are Gillick competent.

An interim NSW Health consent form is located in Appendix 5.6.

2.4 Procedures for capturing and documenting imaging

Standard: There are standardised procedures for capturing and documenting images to reduce variation across statewide services

LHDs/SCHN must support NSW Health workers to comply with 2.4.1 and 2.4.2 below.

2.4.1 Capturing imaging

Capture of imaging in cases of suspected child abuse must be conducted in accordance with the NSW Health Privacy Manual for Health Information, 2015, and must be restricted to NSW Health workers with suitable training and experience in the procedures required to comply with this photo and video imaging policy.
At a minimum, NSW Health workers must:

- Carefully explain to the child or young person, and where appropriate their parent(s)/guardian(s), what the procedure is going to involve in advance of the examination.

- Provide the opportunity for the child or young person, and/or parent(s)/guardian(s) to ask questions and receive answers in a way that takes into consideration the person’s level of development and understanding as described in section 2.1 of this policy.

- Seek informed consent as described in section 2.3 of this policy directive via a process that:
  - Explains what consent means in relation to the separate specific purposes for which images may be used (as described in section 2.3 of this policy directive) and the implications that may arise for the child, young person or their parent/guardian providing consent.
  - Provides options for providing or refusing consent at any time during the course of the examination for:
    - The capture of images of specific areas of the body.
    - The specific purposes for which images may be used.

- Consider whether the child or young person and their parent(s)/guardian(s) would find it helpful if the practitioner or other NSW Health worker demonstrated the use of the video colposcope and observation monitor. This could be achieved by displaying real time magnified images of objects and/or non ano-genital body parts on a monitor placed in a location easily seen by the child or young person and examiner.

- Ensure that images of a child or young person's face are not captured, unless it is required to document a clinical finding.

- Capture the minimum number of images required to adequately document a clinical finding.

- Adopt the following good practice techniques:
  - Use a RAW (digital negative that requires processing), TIFF or JPEG format for capturing still images.
  - Use a procedure that will allow reliable identification of the recording(s) in relation to the particular child or young person and the time that the image(s) was taken. For example, include the child’s hospital ID label for identification purposes.
  - Include some form of further visual identification on the first and last image, including the child’s name or initials, Medical Record Number (MRN) and/or Area Unique Identifier (AUID) and the date.
  - Include a scale in the image, where possible.
  - Consider anterior, posterior and lateral images of the patient and document the anatomical location of each image (an example 'Request for medical photography services' form is located in Appendix 5.7).

When conducting telehealth NSW Health workers must:

- Consider the professional capacity of the host and remote site examiners as either the supervising or the supervised clinician based on their relevant and appropriate training and experience.

- Act in accordance with the requirements of this policy directive.

- Consider using the good practice techniques set out in the Agency for Clinical Innovation Guidelines for the use of telehealth for clinical and non-clinical settings in NSW, 2015.

NSW Health does not support recording of an entire telehealth consultation with a patient or any audio recording.
2.4.2 Documenting imaging

 NSW Health workers must:


- Reference images using an individual health care patient identification system including a child or young person’s name or initials, Medical Record Number (MRN) and/or Area Unique Identifier (AUID), date of birth (DOB), the date the images were captured and the name of the treating physician

- Document consent and the existence of images in the patient's medical records. For physical abuse and neglect the Suspected Child Abuse and Neglect (SCAN) Medical Protocol, 2014 may be used, unless this is being assessed in conjunction with suspected sexual abuse when the Child Sexual Assault Medical Protocol in the Sexual Assault Investigation Kit (SAIK) may be used. Details must include:
  - Any refusal of consent for capturing photo and video imaging
  - Any withdrawal of consent for the capture or use of photo and video imaging before and during the examination
  - The name of the photographer, the date and time, and the location of where the images were taken to maintain integrity in the event of legal action or issuing of a subpoena
  - The number and type of images that were taken

- Note that child abuse and neglect images must be stored securely and separately from a child or young person’s principal health care record (see section 2.6.2) and a reference placed on the health care record where the images are located to identify the existence of any principal health care record or other relevant health related documents. Index or patient administration systems must reference the existence of satellite/decentralised health care records that address a specific issue and that are kept separate from the principal health care record

- Document authorised permission for release/transmission in the patient's medical records (see section 2.6.3 of this policy directive).

Where telehealth is used, document at both sites that the consultation has occurred and ensure that this documentation concurs.

It is good practice to disclose the existence of images to NSW Police Force on the Expert Certificate.

2.5 Devices used to capture, record, store and transmit images

 Standard: Capture, recording and storage of images is limited to LHD/SCHN owned memory devices

LHDs/SCHN must ensure that:

- In cases of suspected child abuse, medical and forensic imaging is captured on dedicated LHD/SCHN owned:
  - Clinical camera imaging devices used for the sole purpose of documenting suspected sexual abuse, physical abuse, and neglect;
    - or where the sole purpose of a clinical camera is not restricted to documenting abuse or neglect, such as in an Emergency Department, the clinical camera must accommodate an LHD/SCHN owned removable memory device and images must be captured onto the removable device and not the camera, using one removable device per patient

56(29/10/15)
Clinical colposcope imaging equipment, preferably used for the sole purpose of documenting sexual abuse

Portable or removable memory devices, such as DVDs, memory sticks and external hard drives

- **Single Lens Reflex (SLR) clinical camera equipment** is the preferred option and:
  - Includes a flash
  - Includes a lens with a close up facility
  - Has at least six megapixels.

A 'stand-alone' personal camera (i.e. one that is not part of a mobile telephone or ipad) may be used in exceptional circumstances and only where:

- No LHD/SCHN owned equipment is available and
- The personal camera can accommodate an LHD/SCHN owned removable memory device and use is restricted to capturing images onto the removable device and not the personal camera, using one removable device per patient.

- All equipment complies with [NSW Health Electronic Information Security Policy](#), 2013 and [NSW Health Privacy Manual for Health Information](#), 2015

- Imaging equipment is:
  - Capable of producing an accurate representation of any evidential clinical finding being recorded
  - Appropriately maintained and managed, such as updating date and time settings recharging/replacing batteries
  - Strictly governed and controlled and adequately secured using lockable facilities
  - Monitored in respect of who accesses and uses it.

- Any equipment or devices used for remote access to NSW Health networks from an external location must be authenticated and authorised by the LHD/SCHN and connectivity must be protected by approved controls. This includes mobile devices, smartphones, tablets, netbooks, notebooks, palmtops, handheld personal organisers, laptops, modems, PDAs, wireless access points, portable or removable storage devices, CD/DVD burners and printers


NSW Health does not support:

- The use of any other personal equipment or devices for the purpose of capturing or storing images in relation to suspected child abuse. Examples include cell phones, smartphones, tablet devices, netbooks, notebooks, palmtop, handheld personal organisers, laptops, USB drives, DVDs and removable memory cards and sticks
- Use of Skype or other insecure software/platforms in NSW Health care settings.

### 2.6 Security and storage of images

**Standard:** Images are stored securely and separately from the principal health care record, to maintain patient privacy

LHDs/SCHN must support NSW Health workers to comply with 2.6.1 to 2.6.6 below.
2.6.1 Transfer of images from the capture equipment to secure storage

NSW Health workers who capture and/or support the management of medical and forensic photo and video imaging in cases of suspected child abuse must:

- Check the original images on the camera equipment/LHD removable memory device and:
  - Consider deleting those where at the time the examiner first views the image(s), in the opinion of the practitioner, it is not usable. For example, the image depicts surrounding context rather than the patient or the lighting or exposure impedes what is depicted. Caution must be exercised and where the practitioner is unsure the image must be retained
  - Delete those where the person that provided consent for imaging withdraws consent before completion of the examination
  - Where images are deleted, document the number of images that were deleted and for each image, the reason why it was deleted
- Transfer the retained original image/s from the capture equipment/LHD removable memory device to LHD/SCHN secure network storage facilities as soon as possible and usually within one working day (see Figure 1)
- Archive retained original image/s. A 'read only' format or the equivalent facility is preferred to ensure the integrity of the original image/s and restrict the potential for editing
- Use a separate working copy of an original image for any editing that might be required
- Check images have successfully transferred to LHD/SCHN secure network storage facilities and then delete images that are left on the camera equipment/LHD removable memory device
- Periodically format capture camera equipment/LHD removable memory devices to ensure data recovery processes cannot be used to recover deleted images: Where a removable memory device per patient is used, such as in personal or non-dedicated cameras, formatting must occur as soon as possible after transfer to LHD/SCHN secure network storage facilities and usually within one working day
2.6.2 Storage of images


Photo and video imaging in cases of suspected child abuse, together with the medical records associated with the imaging, must be stored securely and separately from a child or young person’s principal health care record.

LHD/SCHN secure storage facilities may be within a Child Protection Unit, Sexual Assault Service, an Emergency Department or other LHD/SCHN facility offering medical and forensic examinations.

All original photo and video images and any separate working copies used for editing must be stored on LHD/SCHN owned restricted secure network drives. Such restriction(s) to be determined by the Chief Executive Officer, or officer delegated responsibility for the security of LHD/SCHN medical records relating to cases of suspected child abuse.

Where LHD/SCHN owned restricted, secure network drives are not immediately available, in some remote areas for example, electronic/digital photo and video imaging must be:

• Transferred from the camera equipment/removable memory device to an LHD/SCHN owned laptop using appropriate safeguards, such as password or PIN codes, together with encryption technology (see Figure 1)
• Kept in lockable facilities with restricted access.

It is preferred that original images are stored using a 'read only' format, or equivalent, and images must be maintained in an original state and not subject to processes that cause permanent alteration.

All hard copy images must be stored securely in LHD/SCHN owned lockable facilities with restricted access. Such restriction(s) to be determined by the Chief Executive Officer, or officer delegated responsibility for the security of LHD/SCHN medical records relating to cases of suspected child abuse.

To maintain the integrity of the images in the event of legal action, images must be stored with:

• A copy of the consent form and documentation that includes the name of the photographer, the date and time the image/s were taken, and the location where the images were taken (see section 2.4.2)
• Accompanying documentation that includes a child or young person’s initials, Medical Record Number (MRN) and/or Area Unique Identifier (AUID), date of birth (DOB), the date the images were captured and the name of the treating physician
• A reference that identifies the existence of any other relevant health related records or documents that are kept separately from the images, such as the location of the principal health care record. The images can be linked to the principal health care record via a notation on the principal record that a 'confidential health record exists'.

The restricted access electronic and hard copy storage facilities must have an auditing or tracking procedure that documents:

• Who, other than restricted access workers, views an image
• When an image leaves the location where it is stored and its destination
• When an image is copied and by whom.
2.6.3 Transmission of images

For the purpose of security and patient privacy, NSW Health workers involved in the transmission of medical and forensic photo and video imaging in cases of suspected child abuse must act in accordance with the NSW Health Electronic Information Security Policy, 2013, NSW Government Digital Information Security Policy, 2015, NSW Health: Health Care Records – Documentation and Management policy, 2012 and the NSW Health Privacy Manual for Health Information, 2015 and:

- Restrict access to images as described in section 2.7 of this policy directive
- Obtain authorised written permission to release/transmit a copy of an image from a senior member of NSW Health staff, such as the attending medical and forensic practitioner, health information manager or a senior medical records officer/manager. Archived original image(s) should be retained as described in section 2.6.1 of this policy
- Document the authorised permission for release/transmission in the patient's medical record and:
  - The details of the request for release, including the reason for release
  - The number and type of images released
  - The date
  - The person/recipient to whom the image/s have been released
  - Full details of the address/location that the image/s were sent to.

**Within NSW Health**

- Consideration must first be given to restricted party viewing of the images at the NSW Health source site.
- Where this is not possible and electronic transmission occurs, it must occur:
  - Within NSW Health email
  - From NSW Health email accounts to another recognised NSW Health address
  - Using appropriate safeguards such as encryption technology, password or PIN codes and delivery/receipt confirmations, where available
  - From LHD/SCHN owned computers, equipment or devices or those that are authenticated and authorised by the LHD/SCHN with connectivity protected by approved controls or, through NSW Health Secure File Transfer solutions.

In all cases consider whether it is feasible to remove or abbreviate patient identifiers on the image and in any subject lines whilst the image is in transit in liaison with the recipient.

**External to NSW Health**

Where it is necessary to release images to restricted parties outside NSW Health, such as the court or under rigorously restricted information sharing practices relating to Chapter 16A and Section 248 of the Children and Young Persons (Care and Protection) Act 1998 (see section 2.7.1 to 2.7.4 for details of permitted access):

- Consideration must first be given to restricted party viewing of the images at the NSW Health source site.
• Where this is not possible:
  − Electronic copy/copies on a removable memory device under strict governance and control using appropriate security safeguards such as encryption technology, password or PIN codes, or where this is not possible
  − Hard copy/copies
should be transported sealed in an appropriately robust sealed envelope (or similar package) with a unique number allocated from a register held by the NSW Health source site. The envelope/package should be delivered by hand by an employee of NSW Health, registered post or courier and a receipt should be obtained.
At no time must a portable or removable device be used if it is not securely encrypted and released using these safeguards.
• Where this is not possible it should be noted that electronic transmission of personal health information to destinations external to NSW Health are not considered secure (NSW Health Privacy Manual for Health Information, 2015) and where electronic transmission is necessary, the following must occur:
  − Appropriate safeguards must be used such as encryption technology, password or PIN codes and where available, delivery/receipt confirmations
  − LHD/SCHN owned computers, equipment or devices or those that are authenticated and authorised by the LHD/SCHN with connectivity protected by approved controls must be used.
In all cases consider whether it is feasible to remove or abbreviate patient identifiers on the image and in any subject lines whilst the image is in transit in liaison with the recipient. Images must never be emailed or uploaded via the internet to cloud services. Personal email accounts must never be used to transmit patient information.
• Communication using File Transfer Protocol (FTP), telnet, Mobile SMS, instant messaging and web traffic (HTTP) is not permitted by NSW Health as a secure process for sharing photo and video imaging (NSW Health Electronic Information Security Policy, 2013).

2.6.4 Ownership and copyright

Images, recordings and documentation produced by NSW Health workers in a NSW Health service facility remain the property of the health service, including those taken by visiting medical officers.
Copyright of all recordings is owned by the State of New South Wales through the Local Health District/Speciality Network.

2.6.5 Destruction of images and medical record information

An original image on the camera equipment/device may be deleted in accordance with section 2.6.1 of this policy directive.
In all other cases, NSW Health workers must act in accordance with the NSW Government General Retention and Disposal Authority policy, 2004 (revised, 2011) and retain images for a minimum of 30 years after legal action is completed and resolved (where known), or after last contact for legal access or 30 years after the individual attains or would have attained the age of 18 years, whichever is the longer.
2.6.6 Images received from external sources

With the exception of formal, professional clinical peer group requests, review of an image sent to a practitioner from any other source, for example, a family member, in the context of investigating allegations of child abuse needs to be carefully managed. Offering an opinion on such images needs to be done with caution because the practitioner may be exposed to various risks, including difficulties arising from the quality of the image, uncertainties about the date and time it was captured, the identity of the person depicted in the image(s) and an inability to document a clear chain of evidence. In these circumstances:

- Where a person depicted in an image has not been examined by an appropriate practitioner, a NSW Health practitioner that receives the image must not provide advice based solely on the image.
- The image should be retained as a record of a request for review, stored separately from images that the examiner has captured and include a notation with full details of the request (for example, the source and date) and any response.

2.7 Access to images for relevant purposes

Standard: Restricted access is provided to images, to maintain patient privacy

LHDs/SCHN must ensure that NSW Health workers comply with 2.7.1 to 2.7.5 below.

2.7.1 Permitted access

NSW Health workers who capture and/or support the management of medical and forensic photo and video imaging in cases of suspected child abuse must ensure that access is restricted to:

- Designated NSW Health workers providing treatment to children or young people or involved in their safety who have unique user identification, individual password authentication and permission controls.
- Circumstances where:
  - It is reasonably necessary, and directly associated with the primary purpose(s) of collection and
  - The patient/their parent(s)/guardian(s) would reasonably expect the information to be used for that purpose, or
  - Separate informed consent has been obtained for the purpose of a) teaching and/or b) research activities.
- The patient or their parent(s)/guardian(s), unless release would affect the personal affairs of any person, including a request by a parent or guardian where such access may lead to child abuse or prejudice a child’s physical or mental health. Caution must be exercised and an interpretation and explanation of the clinical findings is preferable to the provision of access to images.
- Approved teaching and/or research activities (section 2.8) where:
  - the young person and/or their parent/guardian has provided separate informed consent, and
  - images are de-identified and anonymity of patients is maintained, and
− the teaching and/or research activities are compliant with the NSW Health Privacy Manual for Health Information, 2015 and other relevant NSW Health policies and the research has received ethical approval (for example, see https://hrep.nhmrc.gov.au/certification/hrecs, http://www.ahmrc.org.au/ethics.php and www.ipc.nsw.gov.au/statutory-guidelines-research-purposes-pdf), and

− electronic and digital information is used in accordance NSW Health Electronic Information Security Policy, 2013 and NSW Government Digital Information Security Policy, 2015

- Quality improvement activities (section 2.9) where:
  - images are de-identified and anonymity of patients is maintained, and
  - Human Research Ethics Committees – Quality Improvement & Ethical Review: A Practice Guide for NSW is used to help to determine the activity, and
  - the quality improvement activities are compliant with NSW Health Privacy Manual for Health Information, 2015 and other relevant NSW Health policies.

- Information sharing under Chapter 16A and Section 248 of the Children and Young Persons (Care and Protection) Act 1998 (sections 2.72 and 2.7.3)

- Requests under a court subpoena (see section 2.7.4)

- The requirements of the Health Privacy Principles NSW Health Privacy Manual for Health Information, 2015.

Where access to images is deemed necessary, consideration must be given to viewing the images at the NSW Health source site.

Where release is deemed necessary it should be restricted to the above circumstances and integrity of security must be maintained in accordance with section 2.6.3 of this policy directive and NSW Health Electronic Information Security Policy, 2013, NSW Government Digital Information Security Policy, 2015, the NSW Health Privacy Manual for Health Information, 2015 and NSW Health: Health Care Records – Documentation and Management policy, 2012.

### 2.7.2 Information sharing under Chapter 16A of the Children and Young Persons (Care and Protection) Act 1998

Chapter 16A establishes a scheme for sharing information relating to the safety, welfare or wellbeing of children and young persons between prescribed bodies.

All applications and requests for access to photo and video imaging under Chapter 16A must be forwarded to an appropriate Health worker, medical and forensic examiner involved in the case, manager of the relevant service that authorised the images to be taken (e.g. Sexual Assault Service, Child Protection Unit, Emergency Department or Paediatric Unit), or LHD/SCHN Central Contact Point, regardless of the author of the recording.

The LHD/SCHN will provide a medical report or Expert Certificate to summarise findings to support investigation, assessment, decision making and coordination of services. Access to images of ano-genital, breast/chest and other sensitive areas of the body must be rigorously restricted and considered in the context that such images can only be interpreted by qualified medical and forensic examiners.

Consideration must be given to the relevance of access to or release of photo and video imaging relating to suspected physical abuse and neglect to prescribed bodies for the purpose of the safety, welfare or wellbeing of the child or young person. Where a request is granted, accompanying interpretation or explanation of clinical findings must also be provided.
Where a medical examination has taken place in accordance with Section 173 of the *Children and Young Persons (Care and Protection) Act* 1998 a medical report is provided for the Secretary of Family and Community Services (FACS). An existing Expert Certificate could also be provided.

### 2.7.3 Information sharing under Section 248 of the Children and Young Persons (Care and Protection) Act 1998

Section 248 governs the exchange of information relating to the safety, welfare and wellbeing of children and young people between the Department of Family and Community Services and prescribed bodies.

Requests under Section 248 should be directed to the LHD/SCHN Central Contact Point and come from the Secretary, Family and Community Services (or delegate).

Under Section 248 FACS can request access to a child or young person's medical record, which includes the Child Sexual Assault Medical Protocol/SAIK and *Suspected Child Abuse and Neglect (SCAN) Medical Protocol*, 2014. The LHD/SCHN will provide a medical report or Expert Certificate to summarise findings to support investigation, assessment, decision making and coordination of services. Access to images of ano-genital, breast/chest and other sensitive areas of the body must be rigorously restricted and considered in the context that such images can only be interpreted by qualified medical and forensic examiners.

Consideration must be given to the relevance of access or release of photo and video imaging relating to suspected physical abuse and neglect to the Secretary of the Department of Family and Community Services and prescribed bodies for the purpose of the safety, wellbeing and welfare of the child or young person. Where a request is granted, accompanying interpretation or explanation of clinical findings must also be provided.

Where a medical examination has taken place in accordance with Section 173 of the *Children and Young Persons (Care and Protection) Act* 1998 a medical report is provided for the Secretary of FACS. An existing Expert Certificate could also be provided.

### 2.7.4 Subpoenas

For the purpose of a subpoena, a 'document' includes 'an electronic medical record or information contained on a computer file, such as photos and/or video' (*NSW Health Subpoenas policy, 2010*) and

For the purpose of this policy directive a photo or video image captured in a case of suspected sexual abuse, physical abuse or neglect, constitutes a 'sensitive record' (section 4.3: *NSW Health Subpoenas policy, 2010*).

LHDs/SCHN must act in accordance with the *NSW Health Subpoenas policy, 2010*, and ensure that the LHD/SCHN designated officer (e.g. medical records health information manager or medico-legal officer or risk manager) is informed about the subpoena, as well as, where possible, the senior health care provider and treating health care provider.

NSW Health workers who manage subpoenas must:

- Be aware of whether any claim for privilege over the images can be applied and take appropriate action
- Follow the precautions for 'sensitive records' (see section 6.4: *NSW Health Subpoenas policy, 2010*)
• Where images are produced, provide only those that are captured under the schedule of the subpoena
• Retain a copy of the subpoena and the images that the Health service provided under the subpoena.

Where the patient whose records are subpoenaed are not a party to the proceedings before the court, the LHD/SCHN must notify the patient:
• That the subpoena has been received
• The date that the photo/video imaging must be provided to the court, so that the patient can arrange to attend court if they so wish.

2.7.5 Sexual assault communications privilege

Records relating to the counselling of victims of sexual abuse may be protected from production to the court. Photo and video imaging is not covered under this privilege (see Chapter 6 of the *Criminal Procedure Act* 1986).

2.8 Use of imaging for teaching and research

LHDs/SCHN must ensure that NSW Health workers comply with the following:

• Specific informed consent must be obtained from the young person or their parent(s)/guardian(s) for de-identified photo and video imaging to be used for a) teaching and/or b) approved research activities. This must include an explanation that consent for future teaching and/or approved research activities may be withdrawn by the person who provided consent or the person depicted in the image(s) once they are Gillick competent.

For this purpose, where consent is provided for de-identified images to be used for the purposes of teaching and/or approved research activities there must be a process to ensure that withdrawal of consent may be withdrawn. An example of good practice is described in Appendix 5.8.

• Anonymity of patients must be maintained during case presentations, demonstrations, teaching, research and at seminars and conferences. Where possible, fictitious data must be used and identification of individuals must not occur. Use of images that would identify the child or young person must not occur. Images of the face must be de-identified and use of blocked sections or cropping, for example, could be used for this purpose.


• Act in accordance with the *NSW Health Privacy Manual for Health Information, 2015*.

2.9 Use of imaging for quality improvement activities

LHDs/SCHN must ensure that NSW Health workers comply with the following:

• Quality improvement activities must:
  − use de-identified images and maintain anonymity of patients, and
  − be determined by reference to *Human Research Ethics Committees – Quality Improvement & Ethical Review: A Practice Guide for NSW*, and
  − comply with *NSW Health Privacy Manual for Health Information, 2015* and other relevant NSW Health policies.
2.10 Maintaining the integrity of images in the longer-term

Standard: The integrity of images is maintained in the longer-term

The extent and range of digital image capturing devices, communication technologies and storage systems create a complex environment and significant challenges and opportunities for those that provide forensic science services and their patients (Australia New Zealand Policing Advisory Agency, 2013).

- LHDs/SCHN must use risk analysis and management techniques to reassess the procedures used for capture, storage, access and security for the purpose of maintaining the integrity of images in the longer term. (See, for example, NSW Health Electronic Information Security Policy, 2013, NSW Government Digital Information Security Policy, 2015, and NSW Health: Health Care Records – Documentation and Management policy, 2012.)

3 REFERENCES


NSW Health PD2010_065. Subpoenas. NSW Ministry of Health. Sydney, NSW.


## 4 Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capture</td>
<td>Capture is the process of recording (acquiring) data, such as an image or video sequence (<a href="https://www.anzpolice.gov.au">Australia New Zealand Policing Advisory Agency</a>, 2013).</td>
</tr>
</tbody>
</table>
| Child Sexual Assault Medical Protocol (the written protocol in the Sexual Assault Investigation Kit (SAIK)) | A written record used by forensic examiners in NSW Health Sexual Assault Services to record all types of sexual abuse examinations for children 0-14 years of age and, where appropriate, may be used for young people 14-17 years, otherwise an adult Medical and Forensic Examination Record (MFER) may be used. It is part of the Child Sexual Assault Investigation Kit (SAIK).

The Adult Sexual Assault Medical Protocol may be used where a young person aged 14 or above attends an adult Sexual Assault Service.

In young people aged 14 to 17, which Protocol is used is contingent upon consideration of the circumstances of the child or young person and whether a child or adult SAIK represents the most appropriate pathway.

The Protocols provide guidance to facilitate the medical and forensic examination of victims of sexual abuse and ensure that laboratory specimens are collected correctly and legal requirements are fulfilled. |
<p>| Children and young people | Child: A person who is under the age of 16 years. Young person: A person who is aged 16 years or above but who is under the age of 18 years. (Section 3, <a href="https://www.legislation.nsw.gov.au">Children and Young Persons (Care and Protection) Act</a> 1998). |
| Colposcope | A lighted, magnifying medical instrument used to examine the tissues of the genitalia. It allows an examiner to take a closer look at a child or young person’s genitalia and check for abnormal areas. Some devices can be fitted with photographic or video equipment that can capture still (photographic) or moving (video) images. |
| Cultural competence | Violence, trauma and neglect occur in culturally diverse contexts. Cultural competence is the ability to identify and challenge one’s own cultural assumptions, values and beliefs. It is about developing empathy and appreciating that there are many different ways of viewing the world, as this is influenced by culture. |
| FACS | Department of Family and Community Services |
| Gillick competence | Whilst parents, or those having parental responsibility rights, generally have the legal authority to provide consent for medical procedures for children and young people under the age of 16 years, the Gillick principle (1985 decision of the House of Lords in Gillick v West Norfolk and Wisbech Area Health Authority and anor) provides that a child’s competence to consent to medical procedures increases as they approach maturity, that is a minor under the age of 16 years may be capable of independently consenting to medical treatment when they have achieved a sufficient level of understanding and intelligence to enable them to fully understand what is proposed. Medical practitioners must decide on a case-by-case basis whether a minor has achieved this level of understanding and intelligence. |</p>
<table>
<thead>
<tr>
<th><strong>HRIPA</strong></th>
<th><strong>Health Records and Information Privacy Act</strong> 2002. The Health Privacy Principles (or HPPs) contained in the HRIP Act establish 15 rules for the management of information.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Intimate image</strong></td>
<td>A photo or video image depicting the genitalia, anus or post-pubertal female breast (<a href="#">Faculty of Forensic &amp; Legal Medicine, 2014</a>) and may also include other parts of the body, such as the buttocks or chest of a pre-pubertal child.</td>
</tr>
<tr>
<td><strong>JIRT (Joint Investigation Response Team)</strong></td>
<td>JIRT is a collaborative partnership between the Department of Family and Community Services, the NSW Police Force and NSW Health workers that jointly manages statutory child protection matters that may require a criminal justice response and a health response.</td>
</tr>
<tr>
<td><strong>JPEG</strong></td>
<td>A digital compression and coding standard (<a href="#">Australia New Zealand Policing Advisory Agency, 2013</a>).</td>
</tr>
<tr>
<td><strong>JRU (JIRT Referral Unit)</strong></td>
<td>JRU is comprised of professionals from the Department of Family and Community Services, the NSW Police Force and NSW Health and ensures that reports of risk of significant harm of children and young people to the Child Protection Helpline that require a child protection response, and may require a health and criminal justice response, are jointly assessed for a response by the three JIRT partner agencies.</td>
</tr>
<tr>
<td><strong>LHD</strong></td>
<td>Local Health District.</td>
</tr>
<tr>
<td><strong>Medical and forensic examiner</strong></td>
<td>A trained Medical Officer, Sexual Assault Nurse Examiner (SANE) or Forensic Nurse who has specialised education and clinical experience in the treatment of children and young people who may have experienced child sexual abuse, physical abuse or neglect and the collection of forensic evidence.</td>
</tr>
<tr>
<td><strong>Medical and forensic examination</strong></td>
<td>A medical and forensic examination is an examination of a patient for the purpose of providing medical care and collecting forensic documentation and evidence.</td>
</tr>
<tr>
<td><strong>Neglect</strong></td>
<td>Where a child or young person’s basic needs (e.g. supervision, medical care, nutrition, shelter and education) have not been met, or are at risk of not being met, to such an extent that it can reasonably be expected to have a significant adverse impact on the child or young person’s safety, welfare or well-being. This lack of care could be constituted by a single act or omission or a pattern of acts or omissions such as failing to attend medical appointments or failing to ensure that a school age child attends school. (<a href="#">Child Wellbeing and Child Protection Policies and Procedures for NSW Health, 2013</a>).</td>
</tr>
<tr>
<td><strong>ODPP</strong></td>
<td>Office of the Director of Public Prosecutions.</td>
</tr>
<tr>
<td><strong>Original image</strong></td>
<td>The first image that is captured onto any media.</td>
</tr>
<tr>
<td><strong>Peer review</strong></td>
<td>The evaluation of work or performance by colleagues in the same field with the aim of maintaining or enhancing the quality of work or performance in that field (<a href="#">Faculty of Forensic &amp; Legal Medicine, 2014a</a>). It includes:</td>
</tr>
<tr>
<td></td>
<td>• Discussion about clinical decision making and interpretation of examination findings and results of investigations</td>
</tr>
<tr>
<td></td>
<td>• Meetings undertaken by and with peers with the aim of updating</td>
</tr>
</tbody>
</table>
knowledge and improving practice through presenting of work to peers for review (Medical Board of Australia, 2014a).

Personal device

A personal device is one which is not owned by a NSW Health Public Health Organisation. Examples of a personal mobile device include a phone, camera, ipad or other tablet and laptop computer.

Photo and video imaging

Photo and video imaging depicts an image that:
Documents the findings of a medical or forensic examination
Is captured, recorded and in some cases, transmitted for clinical or forensic purposes
Exists in live 'real time' or is stored in hard copy or electronic form
Can be transmitted in real time or stored and transmitted at a later point in time
May become evidence in a legal proceeding.

Photo and video imaging can be captured using a camera or video recorder. Both can be used in conjunction with a colposcope to enhance magnification and lighting.

For the purpose of this policy, photo and video imaging constitutes part of a health care record.

Physical abuse

Physical abuse occurs if a child or young person sustains a non-accidental injury or is being treated in a way that may have or is likely to cause injury. The injury may be inflicted by a parent, carer, guardian, other adult or other child or young person. (Child Wellbeing and Child Protection Policies and Procedures for NSW Health, 2013).

Prescribed body

Chapter 16A of the Children and Young Persons (Care and Protection) Act 1998 establishes a scheme for sharing information relating to the safety, welfare or wellbeing of children and young persons between prescribed bodies. A 'prescribed body' is any organisation specified in Section 248 (6), Children and Young Persons (Care and Protection) Act 1998 or in clause 7, Children and Young Persons (Care and Protection) Regulation, 2000, or in clause 8, Children and Young Persons (Care and Protection) Regulation, 2012.

Public Health Organisation

A 'Public Health Organisation' is:
A local health district, or
A statutory health corporation, or
An affiliated health organisation in respect of its recognised establishments and recognised services.


SAIK

Sexual Assault Investigation Kit (see 'Child Sexual Assault Medical Protocol').

SCAN Protocol


SCHN (Sydney Children’s Hospitals)

The Sydney Children's Hospitals Network comprises The Children's Hospital at Westmead, Sydney Children's Hospital, Randwick, Bear Cottage, the
<table>
<thead>
<tr>
<th>Network)</th>
<th>Newborn and Paediatric Emergency Transport Service (NETS), the Pregnancy and Newborn Services Network (PSN) and the Children's Court Clinic.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sexual abuse</td>
<td>The terms sexual abuse and sexual assault are often used interchangeably. For the purposes of this policy directive 'sexual abuse' is used to refer to sexual activity or behaviour that is imposed, or is likely to be imposed, on a child or young person by another person (Child Wellbeing and Child Protection Policies and Procedures for NSW Health, 2013).</td>
</tr>
<tr>
<td>Sexual assault</td>
<td>See 'sexual abuse'.</td>
</tr>
<tr>
<td>Sexual Assault Communications Privilege (SACP)</td>
<td>As set out in the Criminal Procedure Act 1986, the SACP allows courts to exclude evidence that would disclose confidential communications made in the course of a professional or sexual abuse counselling relationship. See Appendix A of the NSW Health Subpoenas policy, 2010, for further information.</td>
</tr>
<tr>
<td>Standard</td>
<td>A standard is a key principle that must be followed.</td>
</tr>
</tbody>
</table>
| Subpoena | A subpoena is an order from a court or tribunal which directs someone that they must on a given date:  
  a) Produce to a court certain (existing) documents for use in legal proceedings  
  b) Attend a court on a particular date to be a witness in a hearing and give evidence, or  
  c) Do both.  
A subpoena can only be issued if legal proceedings have been commenced. For the purposes of a subpoena a ‘document’ includes, ‘an electronic medical record or information contained on a computer file, such as photos and/or video’ (NSW Health Subpoenas policy, 2010). |

References


5  APPENDICES

5.1  List of relevant policy documents

<table>
<thead>
<tr>
<th>Policy Document</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSW Health PD2013_033</td>
<td>Electronic Information Security Policy.</td>
</tr>
<tr>
<td>NSW Health PD2010_065</td>
<td>Subpoenas policy.</td>
</tr>
<tr>
<td>NSW Health PD2005_405.</td>
<td>NSW Health Consent to Medical Treatment - Patient Information policy.</td>
</tr>
</tbody>
</table>

5.2  Related policies and procedures

- Child Sexual Assault Medical Protocol *(2002). *(Often referred to as the SAIK (Sexual Assault Investigation Kit)

Sydney Children’s Hospitals Network and Kaleidoscope Greater Newcastle (SCHN KGN) Clinical Guideline on Photography and Video Recording of Children and Young People under 18 years who are Suspected of Having Been Physically Abused, Neglected or Sexually Abused who Present to any of the Children’s Hospitals in NSW (2012).
5.3 Key related policies and procedures to respond to adult sexual assault:

*Sexual Assault Services Policy and Procedures Manual (Adult), PD2005_607.*


*Clinical Practices – Adult Sexual Assault Forensic Examinations Conducted by Nurse Examiners, PD2005_614.*

5.4 Key Aboriginal health policies and procedures


5.5 Membership of the Photo and Video Imaging Reference Group

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Organisation</th>
<th>LHD/SCHN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Professor Graham Vimpani AM</td>
<td>Chair of the Reference Group Senior Clinical Adviser</td>
<td>Child Protection and Wellbeing</td>
<td>NSW Kids and Families</td>
</tr>
<tr>
<td>Mr David Bennett</td>
<td>JIRT Police Officer</td>
<td>NSW Police Force</td>
<td>N/A</td>
</tr>
<tr>
<td>Ms Sue Burke</td>
<td>District Manager, Sexual Assault Services and JIRT Health</td>
<td>Bloomfield Hospital</td>
<td>Western NSW LHD</td>
</tr>
<tr>
<td>Ms Danielle Clark</td>
<td>Manager</td>
<td>Violence Prevention and Response</td>
<td>NSW Kids and Families</td>
</tr>
<tr>
<td>Ms Lisa Crawford</td>
<td>Senior Analyst</td>
<td>Violence Prevention and Response</td>
<td>NSW Kids and Families</td>
</tr>
<tr>
<td>Mr Paul de Sensi</td>
<td>Medical Photographer</td>
<td>Sydney Children’s Hospital, Randwick</td>
<td>Sydney Children’s Hospitals Network</td>
</tr>
<tr>
<td>Dr Rosemary Isaacs</td>
<td>Medical Director, Sexual Assault</td>
<td>Royal Prince Alfred and Liverpool Hospitals</td>
<td>Sydney and South West Sydney LHDs</td>
</tr>
<tr>
<td>Ms Robyn Lamb</td>
<td>Dept. Head (Allied Health), Child Protection</td>
<td>Sydney Children's Hospital, Westmead</td>
<td>Sydney Children’s Hospitals Network</td>
</tr>
<tr>
<td>Ms Jenny Marshall</td>
<td>Acting Director</td>
<td>Child Protection and Violence Prevention</td>
<td>NSW Kids and Families</td>
</tr>
<tr>
<td>Ms Julia Martinovich</td>
<td>Telehealth Implementation Officer</td>
<td>NSW Agency for Clinical Innovation</td>
<td>N/A</td>
</tr>
<tr>
<td>Dr David McDonald</td>
<td>Senior Staff Paediatrician</td>
<td>Tamworth Rural Referral Hospital</td>
<td>Hunter New England LHD</td>
</tr>
<tr>
<td>Name</td>
<td>Title</td>
<td>Organisation</td>
<td>LHD/SCHN</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Ms Lorna McNamara</td>
<td>Director</td>
<td>Acting Director</td>
<td>Education Centre Against Violence, Child Protection and Violence Prevention</td>
</tr>
<tr>
<td>Ms Petra Milnes</td>
<td>Executive Officer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dr Louise Millward</td>
<td>Senior Analyst</td>
<td></td>
<td>Violence Prevention and Response</td>
</tr>
<tr>
<td>Ms Elena Mirenzi</td>
<td>Manager</td>
<td></td>
<td>Violence Prevention and Response</td>
</tr>
<tr>
<td>Ms Lynn Mitchell</td>
<td>Senior Analyst</td>
<td></td>
<td>Violence Prevention and Response</td>
</tr>
<tr>
<td>Ms Chloe Moddel</td>
<td>Telehealth Implementation Officer</td>
<td></td>
<td>NSW Agency for Clinical Innovation</td>
</tr>
<tr>
<td>Dr Maria Nittis</td>
<td>Department Head, Forensic Medical Units</td>
<td></td>
<td>Blacktown Hospital, Western Sydney LHD</td>
</tr>
<tr>
<td>Mr Hugh Percival</td>
<td>Legal Officer</td>
<td></td>
<td>Legal and Legislative Services</td>
</tr>
<tr>
<td>Dr Anne Piper</td>
<td>Community Paediatrician/Training Adviser, Child Protection</td>
<td></td>
<td>John Hunter Children's Hospital</td>
</tr>
<tr>
<td>Detective S/Sergeant Ian Priest</td>
<td>Staff Officer, Child Abuse Squad</td>
<td></td>
<td>NSW Police Force</td>
</tr>
<tr>
<td>Dr Shanti Raman</td>
<td>Paediatrician/Medical and Forensic Practitioner</td>
<td></td>
<td>Liverpool Hospital</td>
</tr>
<tr>
<td>Dr Carol Stevenson</td>
<td>General Practitioner in Aboriginal Health, Medical Educator, Medical Coordinator</td>
<td></td>
<td>Lismore Sexual Assault Service</td>
</tr>
<tr>
<td>Dr Dimitra Tzioumi</td>
<td>Staff Specialist, Child Protection Unit</td>
<td></td>
<td>Sydney Children's Hospital, Westmead</td>
</tr>
</tbody>
</table>

56(29/10/15)
5.6 Interim NSW Health consent form

Reference should be made to: Child Wellbeing and Child Protection Policies and Procedures for NSW Health, 2013 (PS2013_007); current standards and guidelines for NSW Health Sexual Assault Services; NSW Interagency Guidelines; Suspected Child Abuse and Neglect (SCAN) Protocol (OL2014_012) and the Child Sexual Assault Medical Protocol in the child Sexual Assault Investigation Kit (SAIK).

I understand that:
- imaging may include ano-genital and breast/chest areas of the body. I have the option to exclude imaging of these or other specific body areas and can advise the examiner accordingly.
- photo and video imaging will be stored securely and confidentially by the NSW Health organisation. Photo and video imaging must be held by the NSW Health organisation for at least 30 years and cannot be destroyed until that time has passed.
- photo and video imaging may be viewed by another forensic examiner for the purpose of obtaining a second opinion or for peer review or by other authorised health workers.
- photo and video imaging can be subpoenaed by the court system as evidence. Where these images are used as evidence they may be viewed by the Judge, the Jury, the Defendant, Counsel for both Prosecution and Defence and any other person whom the Judge considers relevant.
- access to photos and video imaging can be requested by and may be released to the NSW Police Force and/or NSW Department of Family and Community Services.

I consent to de-identified copies of my photo/video imaging being used in: (Please tick as applies)
- a) teaching ☐ Yes ☐ No
- b) research ☐ Yes ☐ No

NOTES: Forensic examiners will:
- a) record any discussions and respect any requests made by me to exclude imaging of specific body areas.
- b) inform me that I have the option of withdrawing my consent for the future use of images for teaching and research at any stage, noting that in some cases it may not be possible for images that have already been used for education or publication prior to the withdrawal of consent to be withdrawn from circulation.
- c) inform me that in order to withdraw my consent for teaching and research I must contact the Hospital/Service attended for information on the procedure required.

Forensic examiner to document any special requests made by the patient and/or discussions relating to specific consents for imaging below.

Please tick the relevant option:
- I do ☐ I do not ☐ consent to the imaging and specific requests documented above.

I am the: ☐ Patient ☐ Patient’s Person Responsible ☐ Guardian ☐ Parent ☐ Other ☐

Signature __________________________ Date __/__/____

Family Name __________________________

Given Names __________________________

For Examiner

I am satisfied the person providing consent has both the capacity and authority to consent to the imaging.

Examiner’s name __________________________ Designation __________________________

Signature __________________________ Date __/__/____

Interpreters name __________________________ Designation __________________________

Signature __________________________ Date __/__/____
5.7 Request for Medical Photography Services

Consent must be sought before sending this form to the medical photographer.

<table>
<thead>
<tr>
<th>Request for Medical Photography Services (to be completed by Health Professional requesting service)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requester</td>
</tr>
<tr>
<td>Designation/Department</td>
</tr>
<tr>
<td>Signature (of Requester)</td>
</tr>
<tr>
<td>Type of request</td>
</tr>
<tr>
<td>Case history print</td>
</tr>
<tr>
<td>Digital file</td>
</tr>
<tr>
<td>Colour prints</td>
</tr>
<tr>
<td>Black and white prints</td>
</tr>
<tr>
<td>Video/audio</td>
</tr>
</tbody>
</table>
Name of Reporter/Photographer:
5.8 Good practice example of a process for complying with a withdrawal of consent for de-identified images to be used for future a) teaching and/or b) research activities

For the purpose of complying with a withdrawal of consent for de-identified images to be used for future a) teaching and/or b) approved research activities:

On receipt of consent

– Each de-identified image should be assigned a reference notation
– The reference notation should be recorded in the patient's file
– A register should be:
  ▪ Kept to document and link the reference notation of the de-identified image with the patient file and
  ▪ Maintained for a minimum of 30 years (NSW Government General Retention and Disposal Authority policy, 2004, revised, 2011)
– A copy of the consent must be stored with the de-identified image(s).

On receipt of a withdrawal of consent, for the purpose of compliance and risk analyses, the de-identified image/s must be deleted from:

– Files that are kept and used for the purposes of future teaching and/or research
– Existing training materials, including Powerpoint files, where they are known to exist.
MANAGING MISCONDUCT (PD2018_031)

PD2018_031 rescinds PD2014_042

PURPOSE

This Policy Directive sets out the requirements for managing potential and/or substantiated misconduct by staff of the NSW Health Service and by visiting practitioners. Further guidance and support in managing misconduct are provided by non-mandatory Information Sheets, including flowcharts, checklists and templates, which are available online on the NSW Health intranet site.

MANDATORY REQUIREMENTS

- The protection of an organisation’s patients and clients, including the children for whom it is responsible, is to be the primary consideration when managing and making decisions related to potential and substantiated misconduct.
- Potential misconduct must be treated seriously and an initial review of any apparent or potential misconduct must take place without delay.
- Where an initial review indicates there is a credible allegation or possibility of misconduct, or that the matter involves a child-related allegation, charge or conviction, further action to pursue the matter in accordance with this policy should take place in a timely manner consistent with the requirements of procedural fairness.
- Any ongoing risks related to potential or substantiated misconduct must be identified, assessed, managed, and regularly reviewed throughout the management process, including any requirements arising from the Service Check Register policy.
- Those involved in a potential misconduct process have both the right to confidentiality and the responsibility for maintaining confidentiality, subject always to the overriding need to be able properly to undertake any inquiries or investigation that may be necessary, and to take the action required by this Policy Directive.
- A person who is subject of a misconduct process must be given adequate opportunity to respond to any allegations, adverse findings, and proposed disciplinary action, prior to any final decision being made.
- A person who is subject of a misconduct process must be afforded the right to a support person being present at any interviews. Other support may also need to be offered to all affected persons, where appropriate.
- Any findings made must be based on relevant available information that is established ‘on the balance of probabilities’.
- Any action to be taken as a response to a misconduct finding must be proportionate to the nature of the misconduct, after consideration of any extenuating circumstances, previous work performance and history, and any identified ongoing risks.
- A termination of employment in NSW Health Service following a finding of misconduct will apply to all roles or multiple assignments undertaken as an employee in the NSW Health Service unless the person can show cause as to why this should not occur. NSW Health organisations must provide dismissed staff access to the show cause mechanism outlined in Section 9.3 of the following Procedures.
- Where the appointment of a visiting practitioner is terminated following a finding of misconduct, the relevant Health organisation must notify any other Health organisation(s) where the visiting practitioner also holds an appointment contract to allow them to assess and manage any local risks.
- Any required internal or external notifications concerning potential or substantiated misconduct (such as to registration authorities) must be made without delay in accordance with the relevant statutory and / or policy provisions.
- Appropriate records of all stages of the process (including the initial review and any investigation) and outcomes must be kept and stored securely.
IMPLEMENTATION
This Policy Directive applies to all staff of the NSW Health Service and to visiting practitioners. It does not apply to staff employed in the NSW Health Executive Service, contractors who are not visiting practitioners, or to agency staff, students, volunteers or researchers who are not staff employed in the NSW Health Service. However, where it is decided to conduct an investigation into alleged misconduct by any person in these categories, this Policy Directive may nevertheless be used to guide the process.

Where a complaint or concern relates to a clinician, the NSW Health policy on managing complaints or concerns about clinicians must be consulted.

The following staff have key responsibilities in relation to this Policy Directive:

**Chief Executives** are required to:
- Ensure that this Policy Directive is communicated to, and complied with by staff involved in managing potential or substantiated misconduct.

**Workforce Directorates / Human Resources Departments / Internal Audit Units / Governance or Professional Conduct and Standards units** are required to:
- Ensure provision of information and advice as necessary to support effective implementation of this policy.

**Supervisors / Managers** are required to:
- Comply with this Policy Directive in dealing with all cases of potential and substantiated misconduct.

The Managing Misconduct Policy and Procedures are available at:
WORKING WITH CHILDREN CHECKS AND OTHER POLICE CHECKS  
(PD2019_003)

PD2019_003 rescinds PD2016_047

PURPOSE
This Policy Directive and the attached Procedures outline the mandatory requirements for National Police Checks (NPCs) and Working with Children Checks (WWCCs) for persons already engaged or employed within NSW Health and for persons seeking to be employed or engaged in NSW Health.

This policy includes the requirements of the Child Protection (Working with Children) Act 2012 and the Child Protection (Working with Children) Regulation 2013 for child related workers, together with the requirements of the (Commonwealth) Aged Care Act 1997 for aged care workers and the transition arrangements under the Disability Inclusion Act 2014 for NDIS workers.

SCOPE
This policy applies to all paid and non-paid workers in NSW Health. It includes staff on rotation, overseas applicants, volunteers, students undertaking clinical or research placements, Visiting Practitioners, on-going, temporary or casual appointments, ‘locum’ or agency staff, contract staff, eligible midwives and nurse practitioners appointed to Public Health Organisations otherwise than as employees and honorary appointments.

This policy applies to all public health organisations and all other bodies and organisations under the control and direction of the NSW Minister for Health or the Secretary NSW Health, including the NSW Ministry of Health and Albury Wodonga Health in respect of staff employed in the NSW Health Service and affiliated health organisations in respect of their recognised establishments and services.

MANDATORY REQUIREMENTS
• NSW Health organisations must identify the type of checks required for each position and ensure that workers have the required NPC and WWCC.
• Except for existing staff members or existing volunteers (where specified in this Policy Directive) NPCs are mandatory for preferred applicants to NSW Health, including for Visiting Practitioners and for volunteers. This is in addition to any requirement to have a WWCC.
• The use of the NSW Health NPC Consent Form and Identification Checklist are mandatory for all NPCs lodged through NSW Health.
• NSW Health organisations must manage and assess criminal history identified through NPCs in accordance with this Policy Directive and any requirements specified by the HealthShare’s Employment Screening and Review Unit (ESRU).
• For types of engagements not mandated or so described in this Policy Directive, NSW Health organisations must determine the need for NPCs based on a risk assessment in accordance with this Policy Directive.
• Except in circumstances set out in this Policy Directives, individuals must have a valid WWCC clearance before starting in a child related role requiring a WWCC.
• NSW Health organisations must validate WWCC numbers with the Children’s Guardian for all individuals engaged in child related work in NSW Health.
• For new child related workers, a signed NSW Health Criminal History Declaration stating no criminal history and a WWCC clearance probity flag that indicates no criminal history meet the mandatory requirement for a NPC.
• The use of the Criminal History Declaration and WWCC clearance probity flag may only be used in strict accordance with this Policy Directive.
• NSW Health organisations must have systems in place to ensure that accurate and complete records relating to WWCC validations and Police Checks are maintained accordingly.
• Except for existing NSW Health workers, students attending clinical placements in NSW Health organisations must have a clear Police Certificate or approval to do so from HealthShare’s Employment Screening and Review Unit.
• In accordance with the Child Protection (Working with Children) Regulation 2013, students attending clinical placements are exempt from the requirement to have WWCCs.
• NSW Health organisations must ensure that:
  o aged care workers maintain satisfactory NPCs (renewed every three years)
  o child related workers maintain valid WWCC clearances (renewable every five years)
  o community transport drivers undergo NPCs every three years in accordance with funding arrangements with Transport for NSW
  o NDIS workers have satisfactory NPCs (renewed every four years).

IMPLEMENTATION

Roles and responsibilities

Chief Executives are to ensure their organisation implements this policy.

Workforce Directorates / Human Resource Department are to ensure the provision of instruction, information and training as necessary to implement this policy.

NSW Health Workers are to comply with the mandatory requirements of this policy.

NON-ADMITTED PATIENT DATA COLLECTION: CLASSIFICATION AND CODE STANDARDS FOR REPORTING SERVICES PROVIDED FROM 1 JULY 2016 IN A WEBNAP EXTRACT FORMAT (IB2016_039)

PURPOSE
The purpose of this Information Bulletin is to inform NSW Health service providers and source system administrators of changes to the classification and code set standard for reporting non-admitted patient service provided from 1 July 2016.

KEY INFORMATION

Due Dates for Reporting
Non-admitted patient activity data must be submitted and of acceptable quality by the 10th calendar day of the month after the month the service was delivered.

Patient or summary level non-admitted patient activity reporting
Patient level non-admitted patient activity is to be reported for in scope activity.
Where the requirement to report patient level activity data cannot be met summary level data must be reported.
The following services are only required to report non-admitted patient activity at the summary level.

1. Group immunisation services (Service Type 023 Immunisation – On Mass (no patient level data)
2. Group diagnostic screening services
3. Needle exchange services and supervised injecting room services (including service units classified to Service Unit Establishment Type 11.04 Needle Exchange Allied Health / CNS Unit).
4. Crisis line counselling telephone services.
This data is to be reported by WebNAP, or by mLoad when that capability is provided.
Summary level must not be reported for any service unit reporting activity at the patient level.
There is no longer a requirement to advise the Executive Director, Health System Information and Performance Reporting Branch of the Local Health Districts (LHDs) and Specialist Health Networks (SHNs) intention to decommission summary level reporting for those service units reporting at the patient level.

Reporting of Services with Multiple Providers
When reporting non-admitted patient services in a WebNAP extract via mLoad each individual service provider should be reported, even if two or more providers have the same provider type code.

Occasion of Service Record Identifier
Each occasion of service must be reported with a unique record identifier in the ‘Service Event Record ID’ field. When resubmitting an occasion of service record the same record identifier must be reported so that the original record is identified and updated.
Where a record identifier is not unique within a single submission to EDWARD, mLoad will prevent the entire file from loading.

Data element classifications subject to change
The requirements for reporting non-admitted patient activity to the Non-Admitted Patient Data
Collection will change for the following data elements:
1. Provider Type
2. Setting Type
3. Financial group.

The changes are of the following type:
1. Some new categories will become effective from 1 July 2016
2. Some existing categories will expire on 30 June 2016
3. Some continuing categories have descriptive label changes.

**Implementation**

The classification changes must be implemented for the reporting of non-admitted patient services provided on or after 1 July 2016 where they are reported via a WebNAP extract format.

These changes will require LHDs / SHNs to:
- Modify local source system classifications
- Map the local source system categories to the appropriate WebNAP alias code values
- Modify WebNAP Service Options for the service units reporting summary level data and impacted by the changed classifications

This involves:
- End dating existing service options containing expired reference codes effective 30 June 2016
- Establishment of new service options containing the new reference codes effective from 1 July 2016.

LHD / SHNs must advise and instruct their source system vendors of the changed requirements and any subsequent need to modify systems. Where a source system is shared between multiple LHDs / SHNs; are compliant with a State Based Build; and / or are subject to application support services provided by eHealth NSW, it is the responsibility of each LHD / SHN to ensure the technical implementation of the modified reporting requirements are raised through the appropriate application support mechanisms. This includes:
- The LHD / SHN Application Advisory Group (AAG) representative ensuring that the change requirements are on the AAG meeting agenda, discussed at the AAG meetings and are approved within a time frame that will enable the implementation due date to be met.
- Directing and authorising eHealth NSW to make the application build change by raising the request for change on the State-wide Service Desk and tracking the change through to its delivery.

**Clarification Advice**

The NSW Ministry of Health will provide clarification advice regarding the changed reporting requirements outlined in the attachments. Requests for advice should be directed to the Health System Information and Performance Reporting Branch, NSW Ministry of Health.

**Primary Contact:**
Position: Data Integrity Officer, Non-admitted Activity
Contact: Jill Marcus
Email: jmarc@moh.health.nsw.gov.au
Telephone: (02) 9391 9897
ATTACHMENT 1

Non-admitted Patient Activity Reporting – Changes to Classification and Code Standards for Reporting Services Provided from 1 July 2016 via a WebNAP Extract Format.

This attachment outlines changes to Non-admitted Patient Data Collection (NAPDC) data elements domains, in scope of the existing WebNAP extract, for services provided on or after 1 July 2016.

The final classifications for each data element reported in a code format, incorporating the changes applicable from 1 July 2016, are provided Attachment 2.

The NAPDC WebNAP Data Dictionary in HIRD provides detailed information pertaining to the concepts and classification, including the new and changed category definitions. Links to this data dictionary are provided on the following NSW Ministry of Health Intranet page:


ATTACHMENT 2

Non-admitted Patient Activity Reporting – Classification and Code Standards for Reporting Services Provided from 1 July 2016 via a WebNAP Extract Format.

This document provides the NSW Health State classification and code standards applicable to services provided from 1 July 2016 for data elements in scope of the Non-admitted Patient Data Collection Core Minimum Data Set and reported via the legacy WebNAP patient level extract.

The NSW Health State classification and code standards applicable to services reported in the EDWARD extract format are provided at the following NSW Ministry of Health intranet page:


60(18/8/16)

NON-ADMITTED PATIENT DATA COLLECTION TRANSITION FROM WEBNAP TO EDWARD REPORTING (GL2015_012)

PURPOSE

The purpose of this Guideline is to advise NSW Health non-admitted patient service providers and non-admitted patient activity source system support staff of the changes in requirements involved in the transition from reporting via WebNAP to reporting via the EDWARD.

An understanding of these differences, and the three phases of implementation, is required to reconfigure source system builds and patient level activity extracts, and redesign non-admitted patient activity reporting business processes.
KEY PRINCIPLES

In line with NSW Health’s strategic direction and the significantly increased volumes of non-admitted patient services being reported at the patient level by NSW Health services the Non-Admitted Patient Data Collection will transition to be reported via EDWARD rather than the interim system WebNAP.

The migration of the data collection to EDWARD will have significant benefits for Local Health Districts (LHDs) / Specialist Health Networks (SHNs) and other NSW Health agencies. LHDs / SHNs should expect higher data availability, more efficient data loading and resubmission processes, significantly improved data error reporting functionality and appropriately secured access to activity data.

When reported via EDWARD the non-admitted patient, admitted patient and emergency department activity data will be automatically allocated the appropriate National Weighed Activity Unit (NWAU) and integrated into a single data mart that supports full patient journey analysis utilising the Enterprise Patient Registry unique identifier.

USE OF THE GUIDELINE

In order to minimise the transition burden, requirements have been prioritised across three phases:

- **Phase 1**: Report current scope via EDWARD and decommission WebNAP
- **Phase 2**: Convert source system extracts and classifications to the EDWARD format
- **Phase 3**: Integrate additional reporting requirements for specific clinical streams

The EDWARD Business Implementation (EBI) Program collaborating with the NSW Ministry of Health’s Health Systems Information and Performance Reporting (HSIPR) Branch will establish a small project team to support transition, testing and address queries as they arise during the migration period.

**Phase 1**

Implementation of phase 1 requires LHDs/SHNs to load WebNAP patient level and summary level extracts into EDWARD and to cease reporting to WebNAP.

To support the transition to EDWARD reporting during Phases 1 and 2, a file upload, conversion and transfer tool, the EDWARD mLoad Tool, will be available for LHDs/SHNs to upload patient level and summary level data extracts from source systems in either the WebNAP extract format, or the EDWARD extract format.

The tool will apply the necessary file format conversions to WebNAP extracts compliant with the 2015/16 WebNAP reporting requirements and file format. It will also produce a container header file (based on user inputs) for both WebNAP and EDWARD flat file formats, and transfer files to the EDWARD drop zone where they will be automatically loaded into EDWARD.

During this phase LHDs / SHNs:

1. Must build EDWARD extracts for non-admitted patient source systems that are not yet reporting at the patient level
2. Must commence the reconfiguration of WebNAP extracts such that the source system can report activity directly in the EDWARD extract format
3. May cease reporting summary level data for services reporting at the patient level once reporting through the EDWARD mLoad Tool
4. May commence (or fully implement any) transition steps outlined in later phases.

Phase 1 must be completed by **30 June 2016**, to enable the decommissioning of WebNAP.
Phase 2
Implementation of Phase 2 requires LHDs / SHNs to complete the reconfiguration of WebNAP source system extracts into the EDWARD extract format and source systems to be fully aligned with the EDWARD classification standards.

During this phase any changes effective from 1 July 2016 will also need to be incorporated into the EDWARD extracts.

During this phase LHDs/SHNs may implement Phase 3 implementation steps.

Phase 2 must be completed by 30 June 2017, to enable the decommissioning of the WebNAP patient level file conversion functionality, compliance with 2016/17 reporting requirements and to establish the foundations required for implementation of Phase 3.

Phase 3
Phase 3 involves reporting the additional data elements set aside in the EDWARD extract file format for the integration of other non-admitted patient data collections for specific clinical streams. It will involve decommissioning the legacy extracts and legacy data repositories (such as HIE and other disparate databases).

This phase may only impact selected source systems. For example, radiotherapy sources system would add data elements required for the integration of radiotherapy waiting times and non-admitted patient cancer notifications, while source systems used by Hepatitis, HIV/AIDS and sexually transmissible diseases services would add data elements pertaining to communicable diseases.

Phase 3 is expected to be completed by 30 June 2018, to enable the decommissioning of the HIE and other legacy data repositories and to establish a single comprehensive non-admitted patient data collection.

FURTHER INFORMATION
The NSW Ministry of Health will provide advice and clarifications regarding the requirements for reporting non-admitted patient activity via EDWARD. Requests for advice should be directed to the Health System Information & Performance Reporting Branch, NSW Ministry of Health.

Primary Contact:
Position: Data Integrity Officer, Information Management & Governance Unit
Contact: Jill Marcus
Email: jmarc@moh.health.nsw.gov.au
Telephone: (02) 9391 9897

Escalation Contact:
Position: Manager, Information Management and Governance Unit
Contact: David Baty
Email: dbaty@moh.health.nsw.gov.au
Telephone: (02) 9391 9828

ATTACHMENT

LINK TO COMPLETE GUIDELINE AND ATTACHMENT:
Mandatory Policy

This document states the Department’s policy in relation to intellectual property arising from health research. Compliance with this policy is mandatory. The Minister for Science and Medical Research supports the policy. The policy may be amended or revoked from time to time.

Application

The policy applies to all public health organisations, Area Health Services, Statutory Health Corporations and Affiliated Health Corporations in respect of their recognised establishments and recognised services. Health research means laboratory, pre-clinical and clinical research and development in all its forms.

This policy does not apply to intellectual property which arises in the course of any other endeavour. It does not apply to commissioned works, that is, work that is specifically commissioned or contracted by public health organisations for a fee.

The main points of this policy are as follows:

- It requires public health organisations to establish intellectual property (IP) committees to manage their IP interests;
- It requires employees to notify any IP they create in the course of their employment to the committee;
- It sets up structures to deal with managing IP created by visitors (including visiting practitioners and conjoint employees such as clinical academics);
- It allows for the proceeds of the commercialisation to be shared between the creator(s) of the IP, the department or section of the public health organisation which originated the IP, and the public health organisation on a 1/3, 1/3, 1/3 basis.

1. Introduction

1.1 This policy recognises the value of health research undertaken within public health organisations. It recognises that the acquisition and dissemination of knowledge and skills in the area of research and clinical practice is of major public benefit and a primary role of public health organisations. Occasionally, the outcomes of health research may have a significant commercial value. The objectives of this policy are to:

- encourage health research in the public health system and the acquisition and dissemination of knowledge and skills;
- manage intellectual property with a potential commercial value in a manner which benefits the public health system as a whole;
- foster an environment within which intellectual property issues can be identified and developed; and
- recognise and reward innovation by staff of public health organisations.

2. Definitions

2.1 Intellectual property as it should be understood in this policy is the legally recognised outcome of creative effort and economic investment in creative effort. IP rights are rights to:

- the protection of intellectual activity or the protection of ideas and information that have been created;
control the distribution of such activity, ideas or information;
receive benefits from such activities, ideas or information by way of exploitation and commercialisation;
recognition and acknowledgement\(^1\).

Intellectual property in a broad sense includes:
- inventions, and patents granted in respect of such inventions and applications for such patents;
- unpatented know-how, which comprise an invention or a way of doing something which is not public knowledge;
- confidential information and trade secrets;
- registered and unregistered designs and applications for registered designs;
- copyright;
- circuit layout rights;
- registered and unregistered trademarks and applications for registration of trademarks;
- get-up and trade dress associated with products and services;
- plant variety rights;
- all other rights resulting from intellectual activity in the scientific, industrial, literary or artistic fields; and
- any contractual rights to use or exploit any of these rights.

A brief description of some forms of intellectual property and the nature of intellectual property rights is to be found at Attachment A.

2.2 This policy also uses other defined terms set out below.

“Health research” means laboratory, pre-clinical and clinical research and development in all its forms. This includes:
- development of treatment procedures and methods;
- development of equipment or other goods which may have application in a clinical setting or a public health application;
- biomedical research;
- research and development of pharmaceuticals; and
- epidemiological and research methods.

“Committee” means an Intellectual Property Committee constituted in accordance with section 4 of this policy.

“Creator” in relation to any intellectual property means an employee(s) who made a significant contribution to the creation or invention of the subject matter (eg the work, product or process) in which the intellectual property subsists, or a visitor(s) or student(s) who made a significant contribution to the creation or invention of the subject matter (eg the work, product or process) in which the intellectual property subsists and assigned his or her rights and interests in the intellectual property to the public health organisation.

“Establishment costs” in relation to intellectual property means any costs paid by the public health organisation to establish and develop the intellectual property for protection or commercialisation, once it has been determined by the public health organisation that commercialisation of the intellectual property should take place. Establishment costs do not

---

include costs that the public health organisation would normally have incurred in carrying out
the research as its core function, for example, the costs of employing/retaining the creators in
their regular capacity or providing infrastructure for medical research. Examples of
establishment costs would include:
• any costs paid to consultants or other professionals for advice on commercialisation or
  further development of the intellectual property for the purposes of commercialisation;
• any costs incurred in setting up a commercial vehicle for the purposes of developing or
  commercialising the intellectual property, or any costs paid to third parties for the
  purposes of commercialising the intellectual property, or further developing the
  intellectual property for commercialisation;
• legal costs incurred in relation to the intellectual property or its commercialisation, for
  example, in drafting joint venture agreements, licence agreements or assignments, or
  providing advice on the commercialisation of the intellectual property; and
• any taxes, or similar outgoings to third parties.

“Gross commercialisation proceeds” means all amounts receivable in consideration of the
assignment or licensing of intellectual property rights. These amounts may be lump sum
payments made up-front or periodically, or may be in the nature of royalties payable on the
happening of future events such as product sales.

“Net commercialisation proceeds” means gross commercialisation proceeds received by the
public health organisation, less establishment costs and protection costs.

“Protection costs” in relation to intellectual property means any costs incurred in taking any
step towards obtaining registration or protection of the intellectual property including fees for
preparing and filing patent applications, renewals, extensions, taxes, stamp duty, and legal and
patent attorney’s fees expended in the course of obtaining protection.

“Visitor” means:
• any person providing services at a public health organisation other than as an employee
  in either a remunerated or honorary position (for example, visiting practitioners, visiting
  medical officers, honorary medical officers);
• any person (other than a student) not employed by a public health organisation who
  utilises the resources of a public health organisation at any time (for example, a visiting
  researcher).

3. Application

3.1 This policy applies to all public health organisations within the meaning of the Health Services
Act 1997 (Area Health Services set out in Schedule 1 of the Act, statutory health corporations
set out in Schedule 2 of the Act, and affiliated health organisations in respect of their
recognised establishments and recognised services set out in Schedule 3 of the Act).

3.2 This policy applies to intellectual property which arises, or may arise, from health research. It
does not apply to intellectual property which arises in the course of any other endeavour.

3.3 This policy does not apply to commissioned works, that is, any intellectual property arising
from work specifically commissioned or contracted by the public health organisation for a fee.
The intellectual property in such work is governed by the terms of the commissioning
agreement.
3.4 All public health organisations which are involved in health research must have an intellectual property policy which is consistent with this policy. A public health organisation is involved in health research if:
- any of its employees or visitors carry out health research; or
- it is a party to any agreements, arrangements or collaborations with other bodies to carry out health research.

3.5 A copy of the intellectual property policy of the public health organisation must be provided to:
- all current employees and visitors who are, or may be, engaged in health research;
- all new employees who will be, or may be, engaged in health research, at the commencement of their employment;
- all visitors and students who will be, or may be, engaged in health research at the commencement of their association with the public health organisation.

The policy which is provided to the individuals listed above, must contain a clear statement to the effect that any or all of the provisions contained in the policy, including provisions relating to the sharing of any proceeds from the commercialisation of intellectual property, may be amended or revoked at anytime.

4. Intellectual Property Committee

4.1 Establishment

Each public health organisation involved in health research shall have an Intellectual Property Committee. Some public health organisations which do not undertake a significant amount of health research may:
- agree to utilise the Committee of another public health organisation;
- may constitute an ad hoc committee from time to time; or
- utilise an existing committee to carry out the IP Committee’s functions, such as the research committee, provided that the membership of such a committee is in accordance with this policy.

4.2 Composition

4.2.1 The composition of a Committee is a matter for the public health organisation and may include co-opted members appropriate to the matter under consideration. However, the standing membership is to include:
- the Chief Executive Officer or a senior executive nominated by the Chief Executive Officer;
- the Director Finance of the organisation or senior financial employee nominated by the Director Finance;
- a senior officer in charge of research within the organisation (except that such a senior officer shall not participate in the making of recommendations in relation to research in which he or she is directly involved or has an interest); and
- a person designated by the CEO of the public health organisation.

4.2.2 Specialist legal advice should be available to the Committee, either by having a legal adviser as a member, or by seeking advice as appropriate. Public health organisations may wish to include members with expertise in commercialising intellectual property.

4.2.3 The Committee shall have a secretariat or responsible officer who is available to coordinate the business of the Committee when it is not sitting, and to receive notifications.
4.2.4 Public health organisations may also have staff who are responsible for intellectual property matters within the organisation, such as IP identification, education, encouragement etc. Such staff may be members of the Committee.

4.3 Functions

4.3.1 The functions of the Committee shall include the receipt and consideration of notifications, the provision of advice, and the making of recommendations to the CEO of the public health organisation as set out in this policy. The Committee shall also act as a resource for staff on intellectual property matters, particularly in relation to the provision of advice on prior disclosure (see section 13).

4.3.2 The Committee may delegate any of its functions, except the function of making recommendations to the CEO of the public health organisation regarding protection and commercialisation of intellectual property.

4.4 Records

4.4.1 The proceedings of the Committee, and any records of those proceedings, shall be treated as commercial in confidence, in so far as they relate to the organisation’s intellectual property interests. See section 13 on prior disclosure.

5. Intellectual property created by employees

5.1 Ownership of intellectual property created by employees

5.1.1 As is the case under the general law, this policy mandates that all intellectual property created by employees of a public health organisation in the course of their employment, is owned by the public health organisation.

5.1.2 For the purposes of this policy, intellectual property which is created by an employee through any significant utilisation of the resources of the organisation (eg, funding, other employees, laboratory facilities, equipment, existing intellectual property of the organisation) is taken to be intellectual property created in the course of the employee’s employment. This shall be the case unless the employee has the prior written agreement of the Chief Executive Officer to utilise the organisation’s resources outside the course of his or her employment to perform the work in the course of which the intellectual property was created.

5.1.3 Public health organisations are not to assert ownership of any intellectual property in scholarly books, articles, audiovisuals, lectures or other such scholarly works (unless commissioned by the public health organisation). However, public health organisations may reserve the right to use such works or subject matter generated by employees.

5.1.4 Nothing in this policy shall be taken to detract from the moral rights conferred on creators under Part X of the Copyright Act 1968.

5.2 Notification by employees of intellectual property

5.2.1 An employee of a public health organisation is to notify the Committee as early as possible of the creation, or anticipated imminent creation, of any work, product or process as a result of, or in the course of, health research undertaken in the course of the employee’s employment which may have, or which the employee believes may have, commercial application.
5.2.2 Each notification must be in writing marked “confidential” and must identify:
- the work, product or process in detail;
- each person involved in the creation of the work, product or process;
- the period in which the work, product or process was created;
- the research project or program in the course of which the work, product or process was created; and
- any known details as to the likely commercial significance of the work, product or process.

5.2.3 Notifications are to occur whether the employee is carrying out the research alone or with other employees, or as part of a collaborative research project with visitors or persons from other organisations.

5.2.4 Only one notification need be made where the research is being carried out by more than one employee, or by employees from different areas of the organisation, provided the notification covers the whole of the research and identifies all employees and other persons involved in the research.

5.2.5 In no case is an employee to take steps to apply for any registration of intellectual property created in the course of their employment in his or her own name (eg file a patent application, or lodge an application for registration of a design etc), unless the intellectual property has been assigned to him or her by the public health organisation in accordance with this policy (see paragraph 5.3.7).

5.3 **Role of the Committee on notification**

5.3.1 The Committee shall examine and consider all notifications under paragraph 5.2. If a notification does not contain sufficient information about the work, product or process for the Committee to properly consider the notification, the notifying employee shall provide to the Committee such further information as the Committee requests.

5.3.2 After consideration of each notification, the Committee shall make a recommendation to the CEO of the public health organisation as to whether any steps toward protection and/or commercialisation of intellectual property notified to it should be undertaken. Such recommendation should be made in a timely manner without undue delay. Recommendations as to protection and commercialisation may not be made at the same time, or be decided upon at the same time. A recommendation may be made to take steps to protect the intellectual property, pending a later consideration and recommendation as to commercialisation.

5.3.3 The public health organisation’s approval is not required for every step of the commercialisation process. The public health organisation may approve a general commercialisation strategy, with details of the strategy to be implemented by the public health organisation (or persons engaged by them for that purpose).

5.3.4 Where protection and/or commercialisation is to proceed, the Committee shall consult the creators in relation to appropriate protection and commercialisation strategies.

5.3.5 Prior to taking any step toward protection or commercialisation, the Committee is to ensure that all relevant creators have been identified.
5.3.6 Where there is more than one creator the Committee shall elicit as soon as possible a written agreement from each creator as to the relative contribution of each of them to the creation of the intellectual property.

5.3.7 If the public health organisation determines that no steps be taken toward protection and/or commercialisation of the intellectual property, the Committee is to consider making a further recommendation to the public health organisation that:

- the intellectual property be assigned to the creator(s) on appropriate terms and conditions (including any retention by the public health organisation of a share of the net proceeds of commercialisation appropriately reflecting the effort and risk taken by the creator in such commercialisation); OR

- the intellectual property be retained by the public health organisation, but that the creator(s) be allowed to act as agent for the public health organisation solely for the purpose of seeking commercial partners, with the public health organisation agreeing to participate in negotiations with such commercial partners (if found) regarding commercialisation.

5.3.8 The appropriate recommendation will depend upon the circumstances of the case and the creator should be consulted in this regard.

5.4 Distribution of proceeds of commercialisation

5.4.1 Where intellectual property developed by an employee is commercialised by, or on behalf of, a public health organisation, and such commercialisation gives rise to income or other benefits to the public health organisation, the benefits to the public health organisation shall be dealt with as outlined in section 5.5.

5.5 Formula for distributing proceeds of commercialisation

5.5.1 The public health organisation shall deduct all establishment costs and protection costs expended by the public health organisation as a first call on all gross commercialisation proceeds.

5.5.2 Following deduction by the public health organisation of establishment costs and protection costs any net commercialisation proceeds will be distributed as follows:

- one third to the creator(s) of the intellectual property;
- one third to the department or section of the public health organisation which originated the intellectual property; and
- one third to the public health organisation.

5.5.3 The public health organisation shall divide the one third share of net commercialisation proceeds payable to the creators amongst the individual creators in accordance with the contributions identified by them in the agreement referred to in paragraph 5.3.6. If no such agreement has been made, the public health organisation shall distribute the one third share in accordance with its own reasonable estimate of the relative contributions of each creator. In making such an estimate, consideration should be given to the role of any creators who have left the employ of the public health organisation. The estimate of the Committee shall be final and binding on the creators until such time as an agreement has been reached between them. This must be noted in the deed of release which is required by paragraph 9.1.

5.5.4 Monies paid to employees under this policy shall be paid as income.

21(11/05)
5.5.5 The eligibility of an employee under section 6 is conditional upon the employee having acted in good faith in accordance with the requirements of the intellectual property policy of the public health organisation.

6. Clinical academics and joint teaching hospital/University facilities

6.1 Significant issues arise in relation to intellectual property created by clinical academics, who work in both the University sector and the public hospital sector. Both the relevant university and the public health organisation are likely to have contributed significantly to the remuneration of the clinical academic, as well as providing the clinical academic with resources, support and infrastructure. It will not always be possible to determine which resources were utilised in the creation of intellectual property by clinical academics.

6.2 Similar issues arise in relation to joint teaching hospital/University facilities, where health research may be undertaken jointly by a mixture of University and hospital staff.

6.3 It is in the interests of both universities and public health organisations that issues regarding intellectual property created by clinical academics and at joint facilities be clarified as early as possible in the identification/protection/commercialisation process.

6.4 Public health organisations which have affiliations with universities are encouraged to negotiate fair and equitable agreements as to the rights of respective parties to the intellectual property created in joint facilities or by clinical academics. Such agreements should take into account the rights of creators as set out in both this policy and the university policy, and the equitable contributions of all parties to the creation of the intellectual property.

7. Intellectual property created by visitors

7.1 Ownership of intellectual property created by visitors

7.1.1 The ownership of intellectual property created by visitors will depend upon the terms of any agreements between the visitor (or the visitor’s employer) and the public health organisation. In general, however, intellectual property created by visitors is owned by the visitor or his or her employer (subject to any applicable agreements).

7.2 Agreements with visitors regarding intellectual property

7.2.1 Where a visitor is to use the resources of a public health organisation to carry out research which may result in the creation of commercially valuable intellectual property, it is appropriate for a prior written agreement to be reached regarding the basis upon which those resources are used. Where the visitor is an employee of another body (for example, an independent research institute or a practice company) the agreement will need to be between the public health organisation and that body. Heads of clinical and research departments of public health organisations should ensure that, where visitors are utilising the resources of their department to create potentially valuable intellectual property, the issue of an appropriate agreement is raised with the visitor and referred to the Committee at the earliest opportunity.

7.2.2 The Committee shall provide advice to the CEO of the public health organisation on appropriate agreements between the public health organisation and visitors who utilise the resources of the public health organisation to conduct health research.
7.2.3 Appropriate agreements may include an assignment of intellectual property by the visitor to the public health organisation on certain terms and conditions, or may include terms under which the public health organisation receives a share of the income of commercialisation of the intellectual property. Whether such terms are appropriate will depend upon a number of factors, including:

- the extent and nature of the research;
- the use of the resources of the public health organisation;
- the source of funding of the research;
- the involvement of other public health organisation staff; and
- any other relevant factors.

7.2.4 The visitor (and his or her employer, if any) is to be fully informed and consulted by the Committee when it considers these issues. Before entering into any agreements with a public health organisation regarding intellectual property, visitors should be given an opportunity to seek their own legal advice.

8. Intellectual property created by students

8.1 Students may be involved in health research utilising a range of resources of the public health organisation. Generally, public health organisations should not claim ownership over intellectual property created by students. However, it may be appropriate for public health organisations to assert rights over intellectual property created by students in the following circumstances:

- the intellectual property has been created utilising substantial resources of the public health organisation;
- the intellectual property is created as a result of pre-existing intellectual property owned by the public health organisation;
- the intellectual property has been created by a team of which the student is a member;
- the intellectual property has been created as a result of funding provided by or obtained by, the public health organisation.

8.2 Heads of research departments should be cognisant of any students undertaking health research within their department that may lead to the creation of valuable intellectual property. Appropriate agreements as to ownership should be concluded at that time, considering the same matters as set out in paragraph 7.2.3.

8.3 Where the student is a student of a University with which the public health organisation has an arrangement under paragraph 6.4, the public health organisation and the University may come to an agreement on how to equitably deal with the intellectual property of students, bearing in mind any claims the students may have under this Policy and the intellectual property policy of the University.

9. Payment of monies under this policy.

Where a share in the proceeds of commercialisation of intellectual property is to be paid to creators under this policy, no monies shall be paid unless the creator first signs a written agreement with the public health organisation acknowledging:

- that the creators’ rights to receive monies under the agreement is in full and final satisfaction of any rights or entitlement that the creator has in respect of the commercialisation of the intellectual property;

21(11/05)
• his or her responsibility for any taxation obligations which may flow from the receipt of those monies; and
• that he or she has had the opportunity to seek his or her own advice in relation to the agreement.

9.2 Such agreements should not be signed or accepted by the public health organisation unless it appears to the public health organisation that the creator has been given an opportunity to seek his or her own advice in relation to the agreement.

10. Independent research institutes funded by public health organisations

10.1 Ownership of intellectual property created by independent research organisations

10.1.1 Public health organisations may house, or be associated with, independent research institutes which carry out health research. Public health organisations may support or resource the development of health research by such institutes in a number of ways, including through the provision of research and administrative staff, infrastructure and equipment, or direct funding. Where such institutes are independent legal entities, they will, generally speaking, be the owners of any intellectual property created by their employees (subject to the terms of the Institute’s constitution and any applicable agreements).

10.2 Agreements with independent research institutes

10.2.1 Public health organisations which provide substantial resources to independent research institutes should have in place agreements with the institute which make appropriate arrangements regarding the rights of the public health organisation in relation to intellectual property created by the institute, utilising the resources of the public health organisation.

10.2.2 Such agreements should ensure that the benefits of research undertaken by such institutes and funded or resourced by the public health organisation are preserved for the public health system. This may be achieved in a variety of ways including (but not limited to):
• provisions whereby the public health organisation is the owner of intellectual property generated by the institute utilising the resources provided by the public health organisation; or
• obtaining for the public health organisation a share of the proceeds flowing from the commercialisation of any intellectual property created by the institute utilising resources provided by the public health organisation; or
• ensuring that all proceeds flowing to the institute from the commercialisation of intellectual property are preserved for the continuing research of the institute.

10.2.3 The advice of the Committee may be sought in relation to such agreements.

11. Collaborative research, joint ventures, arrangements with third parties

11.1 Public health organisations may create intellectual property in conjunction with other organisations in the public or private sector, for example, under collaborative research projects or joint venture arrangements for specific research and development projects. The ownership of intellectual property which arises from such ventures will depend upon the contractual arrangements between the parties.
11.2 Where public health organisations enter into collaborative research activities, joint ventures, or similar arrangements with third parties, the public health organisation should ensure that there is a written agreement between the parties which sets out:

- the rights (if any) of each party to use the intellectual property which the other party brings to the project;
- the ownership of any intellectual property created by the research partners, both individually and jointly;
- where valuable intellectual property may arise, the rights and obligations of the parties regarding the protection and commercialisation of the intellectual property;
- the benefits flowing back to each of the parties with respect to any proceeds of commercialisation.

11.3 Any such agreement should protect the interests of the public health organisation proportionately to its contribution to the research project.

11.4 The public health organisation should obtain legal advice regarding proposed agreements on joint ventures and collaborative research projects.

11.5 The requirements of the Public Authorities (Financial Arrangements) Act 1987 in relation to joint ventures must be complied with (including the requirement that joint venture arrangements have the Treasurer’s approval).

12. Commercialisation by outside bodies

12.1 It is recognised that public health organisations may not have the expertise to undertake commercialisation of their intellectual property, and will contract with a third party to do so on their behalf.

12.2 Arrangements of this kind will vary in their terms and conditions, and may or may not involve the following aspects:

- Assignment of the intellectual property to the commercialising entity;
- Provisions for profit sharing with creators (rather than relying on the intellectual property policy of the public health organisation).

12.3 Where such arrangements are entered into, the public health organisation should ensure that the return to the organisation is equitable, and that any profit sharing arrangements with employees do not disadvantage employees by providing a lesser entitlement than that envisaged by this policy. The advice of the Committee may be sought in relation to such arrangements.

13. Need for confidentiality – prior disclosure

13.1 Much health research does not, and is not intended to, lead to commercial application. Researchers, however, should be cognisant of the possibility of research leading to a commercial application. Where a researcher is in doubt as to whether research may lead to a commercial application or have any possible commercial value, the advice of the Committee should be sought at the earliest opportunity.

13.2 The confidentiality provisions set out below do not apply to research which does not have a potential commercial application or commercial value. This policy is not intended to unnecessarily restrict the flow of information in the course of collaboration and communication between researchers and practitioners which this policy recognises is essential in health research.
13.3 Where it is considered that commercially valuable intellectual property has been created (in particular, patentable innovations, know-how or other secret information) it is critical that no disclosure, or publication of such innovation be made to any third party outside the public health organisation, until appropriate steps have been taken to secure statutory protection. Disclosure within the public health organisation should be kept on a “need to know” basis, and all Committees must have procedures in place to ensure that the confidentiality of information presented to them is preserved.

13.4 Prior publication of an innovation can be fatal to the ability to obtain a patent, as it may lead to the loss of “novelty” of an invention, a prerequisite for the granting of a patent. Prior publication can be fatal to a patent, whether the publication is made in Australia or overseas. Prior publication may include verbal and written disclosures made in any forum. The presentation of papers at scientific conferences, the publications of papers in peer journals, and the discussion of the innovation or aspects of it with colleagues who are not under obligations of confidentiality will generally constitute prior publication.

13.5 Where a creator wishes to make disclosure relating to an innovation which has potential commercial value (e.g., a publication or a presentation at a scientific conference), the creator must first seek the permission of the Committee. The Committee can obtain legal advice as to whether the nature of the publication will jeopardise patent or other intellectual property rights, and advise the creator appropriately regarding what disclosures may and may not be made. This advice may include appropriate amendments to the proposed publication or presentation. Researchers should ensure that the advice of the Committee is sought a reasonable time prior to the planned publication or presentation date.

13.6 Public health organisations must ensure that advice on prior disclosure is provided in a timely manner, so as not to unnecessarily prejudice appropriate publication of research results. Students should not be prevented from publishing a thesis under this policy for a period greater than two years.

14. Miscellaneous

14.1 Taxation matters

14.1.1 Public health organisations should ensure that they comply with any relevant taxation obligations which may flow from the commercialisation of intellectual property. Relevant taxation advice may be required in this respect.

14.1.2 Public health organisations should inform employees or visitors who receive a share in the proceeds of commercialisation of intellectual property under this policy that taxation obligations which flow as a result of the receipt of such money are a matter for them and that they should obtain their own taxation advice.

14.2 Audit matters

14.2.1 The audit treatment of any monies received as a result of the commercialisation of intellectual property (either by the Area alone, or as a result of a joint venture or similar arrangement) must be undertaken in accordance with the Department’s Accounts and Audit Determination for Area Health Services and Public Hospitals.
14.3 Risk Management

In commercialising intellectual property, public health organisations are not to incur undue risk of liabilities to the public health system. Legal and risk management advice must be obtained as part of the commercialisation process. Approval for incurring any risks as part of the commercialisation process must be obtained from the Department’s Chief Financial Officer prior to the commercialisation being commenced. No monies shall be paid by a public health organisation to creators of intellectual property where there are any extant risks outstanding to the public health organisation, unless the Chief Financial Officer has given approval in writing. Such approval shall only be given on the basis that the risks have been appropriately managed.

14.4 Variations from this policy

- Any arrangements in relation to intellectual property which depart from this policy must be approved in writing by the Director-General (or delegate). Such variations include:
  - Any profit sharing arrangement which involves employees sharing in commercialisation other than by payment of monies (e.g., through equity in a start-up company);
  - Any profit sharing arrangement that involves creators sharing the proceeds of commercialisation in greater share than envisaged in Para 5.5.2.

14.5 Dispute resolution

Public health organisations should agree on an appropriate dispute resolution process for disputes arising under this policy. Where public health organisations enter into individual agreements for the commercialisation of health research it is recommended that appropriate dispute resolution procedures are included in the agreement.

15. Review of this policy

15.1 It is proposed that this policy be reviewed within a reasonable period after its implementation by the Department of Health. Comments on the operation of this policy by public health organisations are encouraged.
ATTACHMENT A: DESCRIPTIONS OF INTELLECTUAL PROPERTY

This guide is designed to provide a simple outline of some types of intellectual property. It is not intended to be a comprehensive legal guide. The advice of the Committee should be sought for a more detailed understanding.

1. Copyright

There are three categories of protection under the Commonwealth Copyright Act 1968 being:

a) literary, musical, dramatic and artistic works, including adaptations and arrangements of works;
b) films, sound recordings, television broadcasts, radio broadcasts, published editions;
c) performers’ protection (not strictly copyright but included in Copyright Act).

Copyright protection is automatic on the creation of a work. It gives the owner the exclusive right to do various acts in relation to the work, including reproducing the work.

There is no copyright in an “idea”. Copyright protects the author’s particular way of expressing an idea. An example of a work created through health research which may attract copyright would be a manual developed explaining a particular product or process, or diagrams and charts explaining a product or process. It is the expression of the product or process which is protected by copyright law, not the product or the process itself. Copyright law only gives protection against the copying of the work and does not protect against the independent creation of a similar work.

Moral rights also exist in relation to literary, musical, dramatic and artistic works and in relation to cinematograph films. Moral rights seek to protect the individual creator’s honour and reputation.

2. Patents

A patent is a right granted in respect of a method, process, device or substance that is new, inventive and useful. Patents are regulated by the Commonwealth Patents Act 1990. If it can be shown that the invention was already known publicly or that it was the subject of an earlier patent, a patent will not be granted. A patent gives the owner the exclusive right to commercially exploit the invention. Unlike copyright, a patent must be applied for and protection is not automatic.

Patent rights are extremely fragile and can easily be lost if the nature of the invention is disclosed, published, sold or otherwise commercialised before a patent is applied for.

3. Registered Designs

Industrial designs can be protected by registration under the Commonwealth Designs Act 1906. The visual appearance of articles is protected – a distinctive shape, configuration, ornamentation or pattern. This protection may protect a design in relation to all sorts of items eg computer keyboards, furniture, toys and spare parts. A design must be new or original in order to be registered. It will not be possible to obtain a registration where there has been prior publication or use of the design. A design registration gives the exclusive right to apply the design to the article in respect of which the design is registered.

4. Trade Marks

The relevant legislation is the Commonwealth Trade Marks Act 1995. A trade mark is a sign used to distinguish goods or services dealt with or provided in the course of trade by a person from goods or services so dealt with or provided by any other person. Trademarks include letters, words, names,
signatures, numerals, devices, brands, headings, labels, tickets, aspects of packaging, shape, colour, sound, scent or any combinations, eg “Vegemite”. Registration can be applied for under the Trade Marks Act. A registered trade mark gives the exclusive right to use the trade mark for the goods or services for which it is registered.

5. Trade Secrets

The protection of trade secrets is an aspect of the law of confidential information and this law tends to be used when traditional areas of intellectual property provide no relief. Trade secrets include manufacturing techniques, customer lists, engineering designs, marketing procedures and some government information.

Employees owe a duty of confidentiality to their employer. This does not mean that information cannot be transferred from one scientist or researcher to another. However, if the information is particularly sensitive or relates to potentially valuable intellectual property, the secrecy of the information can be maintained and protected by confidentiality agreements. Confidentiality is an important concept and is useful in research and development. It can be used to assist the flow of scientific or medical information while maintaining legal secrecy and safeguarding patenting rights.

6. Circuit Layout Rights

Circuit layout rights protect original layout designs for computer chips and integrated circuits. The owner of an original circuit layout has the exclusive right to copy and commercially exploit the layout in Australia. Protection is automatic.
STATE HEALTH FORMS (PD2009_072)

PURPOSE

This policy and attached procedures define the processes for the creation and management of State Health Record Forms incorporated in Health Care Records.

The scope of the policy is to have clinical statewide forms filed in the Health Care Record and the standardisation of the physical Health Care/Medical Record Cover as well as other health record documents such as labels and dividers. This policy includes but is not limited to Inpatient facilities, Community Health Centres and outpatient clinics/areas.

MANDATORY REQUIREMENTS

Health services are required to use standardised forms developed by the NSW Health State Forms Management Committee.

All State Health Record Forms for inclusion (or potential for inclusion) in the Health Care Record must be approved by the NSW Health State Forms Management Committee (SFMC) or Health Service forms for use only within the Health Service must be endorsed by the local forms committee.

Health Services must establish:

- A functional health service Health Records Forms Committee
- Processes to ensure all line managers are accountable for the effective implementation of standard health record forms across the health service, including Directors of Clinical Operations, Clinical Governance and Nursing and Midwifery Services, Health Information Management units and facility based Health Information services.

All NSW Health State Record forms can only be obtained from the State Print and Print Management contracted supplier.

IMPLEMENTATION

The Health Service Chief Executive is responsible for:

- Establishing a functional health service Health Records Forms Committee, a member of which must act as representative to the NSW Health State Forms Management Committee (SFMC).
- Establishing processes to ensure all line managers are accountable for the effective implementation of standard health record forms across the health service, including Directors of Clinical Operations, Clinical Governance and Nursing and Midwifery Services, Health Information Management units and facility based Health Information services.

The Health Service Records Forms Committee is responsible for:

- Reviewing clinical forms intended for statewide use.
- Approving all clinical forms to be used by its Health Service.
- Ensuring all clinical forms meet the requirements of relevant Australian Standards (e.g. AS2828), NSW Health Policy Directives, a Health Service and State Health Records Forms templates.
- Working with the NSW Health, appointed Print and Print Management Services contracted provider, to facilitate Statewide implementation of the Policy.
To standardise clinical forms across their health service where possible.
To provide a formalised communication network between Health Service forms users, Executive, the contracted Print Management Services provider and the SFMC.
To make recommendations for ongoing introduction/amendment/deletion of forms.
Ensuring that the terms of reference includes a requirement that direct clinical contribution is obtained as required.

The custodians and authors of Health Records Forms (including the NSW Department of Health) are responsible for:

- Ensuring all steps in the health record forms development processes adhere to policy.
- Submitting relevant forms through their health service representative to the SFMC for review and endorsement.
- If NSW Health Policy Directive or Guideline requires a Health Record form to be used or created in order to comply with that policy or guideline the form must be submitted directly to and processed through the NSW Health SFMC and form a part of that Policy Directive or Guideline before it is distributed for implementation.

Health Support is responsible for:

- Monitoring and Reporting:
  - Supplier (Print and Print Management Services) performance
  - Quality issues (product, artwork and supply)
  - Health Service usage and expenditure
  - Health Records Forms gallery
- Management and support of the SFMC.
- Implementation of a Communication Plan.
- Collaboration with Health Item Master File program.
- Maintenance of the State Health Record Forms and bar-code number allocation register.
- Management of print supplier contract and meeting costs associated with contract, (e.g. destruction of obsolete forms etc).

Persons undertaking the evaluation of forms are responsible for:

- Confirming that the form is compliant with the current Australian Standards on Hospital Medical Records (AS2828).
- Ensuring the form has a consistent format and template.
- Ensuring that the form meets the criteria as per stated throughout the Appendices to this policy.
- There is clear evaluation criteria against which the form is to be evaluated.
- A diverse group is selected to evaluate where applicable and possible and that consultation with any Health Service which is taking part in the evaluation has been consulted with at the highest level.
- Evaluation report is clearly documented and that any changes made to a form are within the boundaries of any policy directive which the form maybe written from.
- That any change which is outside a policy within which the form has been written from is referred back to the content owners for approval.
- That the form is in and remains in State Forms Management Committee State forms template.
1. BACKGROUND

1.1 About this document

In line with the strategic reform initiative, NSW Department of Health has instructed Health Support Services to include forms rationalisation and print management across NSW Health. This project will ultimately cover all forms however initially health records rationalisation is being addressed.

It is estimated that there are approximately 15,000 commercially printed health record forms being used across NSW Health. There is not a common Statewide process to develop or review health (clinical) record forms. Not all forms comply with current Australian standards (e.g. AS2828). NSW Department of Health develops policies and guidelines with health records forms incorporated for implementation across NSW Health without always making provision for:

- A co-coordinated implementation plan across all Health Services and agencies
- Compliance with the current Australian Standards (i.e. for paper-based health care records - AS2828)
- Review of the printing and distribution requirements and impact across all Health Services and agencies.

1.2 Key definitions

Health Record Form: A record of the provision of care, assessment, diagnosis, management and/or professional advice given to a person. This term is used interchangeably with clinical form. A Health Record Form is a Clinical form that is endorsed by Health Service Forms Committee for use within the area/service.

State Health Record Form is considered to be a:

- Clinical Form that is mandated by NSW Department of Health for statewide usage. See appendix 3 for the Statewide forms templates.
- Clinical Form that Health Services have devised for health service or agency use.
- Clinical Form that has undergone a NSW Health State Forms Management Committee (SFMC) approval process.

Health Care Record: A Health Care Record is a documented account of a patient’s/client’s health evaluation, diagnosis, illness, treatment, care, progress and health outcome that provides a means of communication for all health care personnel during each visit or stay at a health service. It is the primary repository of all information regarding patient/client care.

The record is used to care for the patient/client during an episode of care but may also be used for future episodes of care, communication with external health care providers and regulatory bodies, planning, research, education, financial reimbursement, quality improvement and public health. The health care record may also become an important piece of evidence in protecting the legal interests of a patient/client, clinician or Health Service.

The health care record may be in hard copy, electronic or other form, and unless otherwise indicated, the provisions of this policy directive apply equally to all health care records regardless of the media in which they are kept.

Health Service: a Health Service within the boundaries of the Health Service Act 1997 (which includes Area Health Services/Chief Executive Governed Statutory Health Corporation, Board Governed Statutory Health Corporations, Affiliated Health Organisations - Non Declared, Affiliated Health Organisations - Declared, Public Hospitals).
SFMC: NSW Health State Forms Management Committee.

Site: Physical facility or service e.g. Hospital, Community Health Centre, Renal Service, Justice Health site.

Location: Ward, Oral Health, Clinic, Unit e.g. ICU, ED.

1.3 Rationale

The introduction of statewide health records forms will assist in:

- Promoting quality processes through
  - Consistent business practices when designing and implementing clinical forms across NSW Health.
  - Statewide standardised document control for all Health Record Forms included in NSW Health Policies.
- Health Services and agencies transferring to electronic medical records systems.
- Streamlining the implementation of NSW Health Policy and forms at the Health Service and agency level.
- Supporting scanning of health care records, including a standardised bar-coding system and the maintenance of a State Health Record Forms Register.
- Promoting effective and efficient work practice by:
  - Decreasing the workload at Health Services and Agencies, who are currently responsible for the implementation of forms incorporated in NSW Health policies and guidelines.
  - Standardising information and formatting to assist staff across NSW Health to accurately and consistently collect patient information, regardless of the health care facility or service.

2. NSW Health State Forms Management Committee

2.1 Terms of Reference

The Committee has the following Terms of Reference:

- Co-ordinate the development of State Health Record Forms and documents.
- Standardise State Health Record Forms and documents and across the whole of NSW Health where possible.
- Ensure compliance with relevant Australian Standards where appropriate.
- Ensure liaison and co-ordination with the Electronic Medical Records Project (eMR) and other related electronic information systems.
- Provide a formalised communication network between form users, NSW Department of Health, Health Support and the contracted Print and Print Management Services Supplier.
- Disseminate forms and related information across NSW Health.
- Approve statewide health record forms and allocate a unique form number.
- Oversee the maintenance of the State Health Record Forms Register.
- Ensure actions and issues are assigned to the appropriate personnel either within Health Support, Health Services/Agencies, NSW Department of Health or the contracted Print and Print Management Services Supplier.
- Regularly review the statewide electronic forms web-site, when developed, for accuracy and initiate remedial action as required.
- Make recommendations for ongoing introduction/amendment/deletion of forms.
- To complement existing Health Service Forms Committees to ensure only endorsed approved (local or state) health record forms are produced for filing in the Health Care Record.
2.2 Governance

The Committee will be responsible to the Deputy Director-General, Health System Support.

2.3 Representation

NSW Health Services (NSCCAHS/HNEAHS/SESIAHS/SSWAHS/SWAHS/GSAHS/GWAHS/ NCAHS/CHW and Justice Health)

Health Support

By Invitation as required
- Standards Australia representative
- NSW Department of Health representative
- eMR Project Team representative
- Ambulance Service NSW representative
- MH-OAT representative
- Print and Print Management Services Contractor representative
- Other persons involved with special projects involving clinical forms and health records

3. Development of Statewide Health Record Forms

3.1 Identification of need for new or revised health record forms

Sources for identifying the need for the development or revision of a State Health record form include, but are not limited to:
- State executive sources including legislative requirements, NSW Health Policy Directives, Guidelines, Australian Standards and specific industry requirements, better practice or research evidence
- Service reviews, Incident Information Management System (IIMS), complaints, root cause analysis (RCAs) and peer review
- Internal and External audit reports

3.2 Development Stage

Custodians and authors of proposed State Health Record forms are required to:
- Search for an existing or similar form.
- Source relevant documentation where possible and ensure forms comply with Best Practice, both in forms design and clinical practice.
- Ensure compliance with NSW Health policy directives, guidelines and information bulletins.
- Ensure there is endorsement from Health Services and supply confirmation of this in writing to the SFMC.
- Ensure that the form utilises the SFMC Forms Template.
- Contact relevant Health Service Forms Committee to identify which form is to be replaced and provide reasons for replacement.
- Through their SFMC representative, send an electronic version of the form and completed application package for approval to the SFMC – see appendix 7 for application checklist.
- Consider usage when stock numbers are being established.
- Specify colour, print and other specifications at the time of form submission.
- Comply with relevant Australian Standards (e.g. AS2828).
• Ensure forms are developed in liaison with appropriate clinical representation at both State and Area level.
• Ensure forms meet medico-legal requirements.
• Ensure relevant stakeholders are alerted to form development.
• Ensure training and/or implementation guidelines and materials are developed and distributed to appropriate Area representatives prior to the introduction of the form.
• The AHS is to establish a single line of communication with the SFMC; and the process for submission to the SFMC should confirm the above has been undertaken and the proposal endorsed at an Area Health Service level, prior to submission.

3.3 Considerations

The impact of creating new Health Record forms is to be considered. This impact may include:
• Increased staff work load due to staff completing the form and Medical Record/Clinical/Health Information Department filing the form.
• Increased size of medical records, which may impact on storage space and have potential OH&S issues due to the weight.
• Costs – for example the colour of form or print, NCR paper, A3 size and booklets.

Instructions/protocols/checklists should not, as a general rule, be included on the back of forms. Rather, alternate approaches should be explored to minimize interference with clinical documentation and unnecessary space requirements in the health care record. For example, instructions can be laminated and placed in an obvious area when introducing the form and/or be included in a procedure.

Only Health Record forms endorsed by the SFMC (or Health Service Forms endorsed by the local Forms Committee) will be filed in the Health Care Record. If a Health Record form is released for use without an authorized form number and bar-code identifier when one is required, then it will be deemed ineligible to be filed into the Health Care Record.

Revised forms, once approved, will be printed for use when the current supply is depleted. If a form is deemed to pose a clinical risk it is to be destroyed at the contracted printers and the artwork removed.

Photocopying of blank State Health Record forms for use and filing in the Health Care Record is not permitted.

3.4 Validation Stage

The NSW Health State Forms Management Committee (SFMC) will review the proposed Health Record form based on the following criteria:
• Form must comply with NSW Health State templates and current Health Record Standards (e.g. AS2828).
• A unique form number must be allocated from the State Forms Register.
• A bar code identifier must be allocated based on the determined state form number.
• Working with the NSW Health contracted Print and Print Management supplier, to manage printing of the form using the approved SFMC template.
• Informing author or custodian of approval or non-approval
• Managing the gallery of State Health Record Forms.
• Provide support to authors in design and concepts (e.g. colours of print, paper, scanning requirements).
3.5 Consultation Phase

A consultation phase will occur for a two week period from the time the form is released to the AHS’s or relevant Health Bodies for comments to be received back.

3.6 Evaluation Criteria

All Health Record Forms will be evaluated on:
- best practice through
  - Consistent format and standardised template.
  - Compliance with current Australian Standards on Hospital Medical Records (AS2828)
- provision of supporting policy and guidelines
- current clinical policy
- clinical work flow
- financial resources
- implementation requirements and the provision of training materials
- decrease in duplication of data items
- decrease in space requirements of health records i.e. storage requirements.

The evaluation process shall include consultation with the Health Services.

3.7 Transition Period

Implementation

High usage clinical forms will be identified for standardisation into the NSW Health statewide template. It is expected that this is where the greatest impact should be gained for cost saving and standard work practice. Examples of these forms are; Medical record covers, Progress notes, Fluid Balance charts, etc.

Phased Transition

The SFMC will determine based on usage and/or clinical criteria the priority for the standardisation of Statewide forms. If more than one form exists then there will need to be consultation with the key stake holders via the members of the SFMC about the design of the most clinically functional and cost effective solution.

Once the SFMC has developed a new form the Print Management Services vendor will be advised not to replace current stock of previous old forms. When the stock is low or no longer available the “Flag” on the Print Management Services vendor’s web site will direct users to the NSW Health Statewide standardised form that must be used.

The replacement Statewide form must be available on the Print Management Services vendor’s web site before old stock is depleted to ensure continuity of supply.

If old stock is still available after 6 months the Print Management Services vendor will identify this issue with the SFMC for a decision to either:
- Contact the owner of the form and advise them of “The option to write off old stock”.
- Make the stock redundant.
- Discuss with the relevant Health Service to determine who will bear this cost.
The Option to Write Off Old Stock

If a Health Service or NSW Department of Health Division needs to write off excess “old” stock (in order to introduce “new” stock rapidly), they must be advised that:

a. The Service Level Agreement Contract allows that the Print Management Services vendor is responsible for the (write off) cost of the first 3 months of stock held.
b. The Health Service would be responsible for the cost of the remaining (unused) “old” stock, and the costs of destruction.
c. Where there is stock held which has not moved in the last 12 months, the Print Management Services contractor would notify the owner of the stock of their intent to write off and destroy (noting the above incurred costs), unless advised otherwise within 2 months time.
d. If no response or advice is given after that period, then the stock will be written off and the entire cost of the stock and destruction costs will be invoiced to the initiating source.

State Mandated Forms (those included in a NSW Health Policy Directive)

a. If the form is Print on Demand (POD), it can be transitioned to the NSW State Forms Template immediately as there is no stock on hand.
b. If the form is warehoused existing stock will be run out and the form transitioned into the NSW State Forms Template ready to be printed on the next reprint.
c. New forms required by Policy Directives in the process of formulation will follow the requirements of this policy elsewhere described.

3.8 Health Record forms that require a trial

The following guidelines are to be followed for introduction of a new State Health Record Forms which are not available in the NSW Health Print and Print Management Contractor’s State Health Record Forms Library:

a. Complete the request and forward it to the Health Service Forms Committee Representative advising of the need to develop/introduce a State Health Record Form. See Appendix 7 for the Application Checklist.
b. The Health Service or agency Forms Representative is to advise the NSW Health State Forms Management Committee (SFMC) Convenor of the proposed form.
c. The SFMC is to formulate the appropriate Working Party who will be responsible for co-ordinating, providing education and supervising the form trial.
d. The time period required for the trial of a form will be dependent on the usage of form. For forms that have a high usage, a minimum trial period of up to 3 months may be required, whilst forms that have a low usage may require up to a 12 month trial period.
e. During the trial period, stocks of the “old” form (if a revised form) must be withdrawn from circulation, to enable a true and accurate trial of the “new” form to occur.
f. All trial forms to adopt the State Forms Template and to be allocated a ‘Trial State Forms Number category and bar code’.
g. At the end of the trial period, the outcome of the trial must be evaluated to determine whether the new form has been accepted by users (results of a compliance audit). If the trial is unsuccessful the current version should be deleted from the State Health Record Forms website as a State form or re-designed. If a local area wishes to continue using the trial form they must give it a local form number.
h. The final form to be registered with State Forms Number, category and barcode.
3.9 Low Usage Forms

Those forms that are identified by the SFMC as extremely low usage can be made available via the relevant website (primarily the NSW Health authorised Print and Print Management suppliers’ website). These forms can be viewed and printed direct from the website. These forms must adhere to this policy including usage of the approved NSW Health clinical forms artwork and must be approved by the NSW Health SFMC. As identified by the SFMC by usage at the present time this is expected to be in the realm of 100 per annum per site.

4. REFERENCES

4.1 External

Australian Standard AS2828 - Paper Based Health Care Records

4.2 Internal

Electronic Information Security Policy – NSW Health (PD2013_033)
Health Care Records – Documentation and Management (PD2012_069)
NSW Health Patient Matters Manual

4.3 Glossary

SFMC = NSW Health Statewide Forms Management Committee
HIMS = Health Information Managers
HS = Health Service
PD = NSW Health Policy Directive
POD = Print On Demand
HSS = Health Support
MHOAT = Mental Health Outcomes Assessment Tool

4.4 Appendices

Appendix 1 - Forms Committee Process and Procedure
   a – State Health Care Record Form Process – New Form Process
   b – State Health Care Record Form Process – Targeted Form standardisation
Appendix 2 - Health Forms Design
Appendix 3 - State Forms Templates
Appendix 4 - State Health Care Record Cover Artwork
Appendix 5 - Terminal Digit Colours for Health Care Record Covers
Appendix 6 - Strip Colours and Patterns
Appendix 7 - NSW Health State Health Record Form Design Checklist
HEALTH CARE RECORDS – DOCUMENTATION AND MANAGEMENT (PD2012_069)


PURPOSE

The purpose of this policy is to:

- Define the requirements for the documentation and management of health care records across public health organisations (PHOs) in the NSW public health system.
- Ensure that high standards for documentation and management of health care records are maintained consistent with common law, legislative, ethical and current best practice requirements.

MANDATORY REQUIREMENTS

Documentation in health care records must provide an accurate description of each patient/client’s episodes of care or contact with health care personnel. The policy requires that a health care record is available for every patient/client to assist with assessment and treatment, continuity of care, clinical handover, patient safety and clinical quality improvement, education, research, evaluation, medico-legal, funding and statutory requirements.

Health care record management practices must comply with this policy.

IMPLEMENTATION

Chief Executives are responsible for:

- Establishing mechanisms to ensure compliance with the requirements of this policy.
- Ensuring health care personnel are advised that compliance with this policy is part of their patient/client care responsibilities.
- Ensuring line managers are advised that they are accountable for implementation of this policy.
- Ensuring implementation of a framework for auditing of health care records and reporting of results.
- Ensuring health care records are audited and results reported within the PHO.

Facility/service managers are responsible for:

- Ensuring the requirements of this policy are disseminated and implemented in their hospital/department/service.
- Ensuring health care personnel within their facility/service have timely access to paper based and electronic health care records.
- Monitoring compliance with this policy, including health care record audit programs, and acting on the audit results.

Health care personnel are responsible for:

- Maintaining their knowledge, documentation and management of health care records consistent with the requirements of this policy.
- Ensuring they are aware of current information about the patient/client under their care including where appropriate reviewing entries in the health record.
1. **OVERVIEW**

1.1 **Introduction**

This standard sets out the requirements for documentation and management for all models of health care records within the NSW public health system. Health care records promote patient safety, continuity of care across time and care settings, and support the transfer of information when the care of a patient/client is transferred e.g. at clinical handover, during escalation of care for a deteriorating patient and transfer of a patient/client between settings.

1.2 **Key definitions**

<table>
<thead>
<tr>
<th>Attending medical practitioner</th>
<th>Visiting Medical Officer or Staff Specialist responsible for the clinical care of the patient for that episode of care.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved clinician</td>
<td>A clinician, other than a medical practitioner, approved to order tests e.g. Nurse Practitioner.</td>
</tr>
<tr>
<td>Health care personnel</td>
<td>A person authorised to provide assessment, diagnosis, treatment/care, observation, health evaluation or professional advice or those personnel who have access to the patient/client health care records on behalf of the NSW public health system to facilitate patient/client care. Health care personnel include clinicians (and students) and clinical support staff. Clinicians include registered health practitioners and others including Assistants in Nursing, social workers, dieticians, occupational therapists and Aboriginal Health Workers. Clinical support staff include Health Information Managers, Clinical Governance and Patient Safety staff, ward clerks, health care interpreters and accredited chaplains.</td>
</tr>
<tr>
<td>Health care record</td>
<td>The main purpose of a health care record is to provide a means of communication to facilitate the safe care and treatment of a patient/client. A health care record is the primary repository of information including medical and therapeutic treatment and intervention for the health and well being of the patient/client during an episode of care and informs care in future episodes. The health care record is a documented account of a patient/ client’s history of illness; health care plan/s; health investigation and evaluation; diagnosis; care; treatment; progress and health outcome for each health service intervention or interaction. The health care record may also be used for communication with external health care providers, and statutory and regulatory bodies, in addition to facilitating patient safety improvements; investigation of complaints; planning; audit activities; research (subject to ethics committee approval, as required); education; financial reimbursement and public health. The record may become an important piece of evidence in protecting the legal interests of the patient/client, health care personnel, other personnel or PHO. The health care record may be paper, electronic form or in both. Where a health care record exists in both paper and electronic form this is referred to as a hybrid record. Where PHOs maintain a hybrid record health care personnel must at all times have access to information that is included in each part. This policy applies to health care records that are the property of, and maintained by, PHOs, including health care records of private patients seen in the PHO. The policy does not apply to records that may be maintained by patients/clients and records that may be maintained by clinicians in respect of private patients seen in private rooms.</td>
</tr>
<tr>
<td>Must</td>
<td>Indicates a mandatory action required by a NSW Health policy directive, law or industrial instrument.</td>
</tr>
</tbody>
</table>

---

36(10/01/13)

---

3 Health practitioners registered under the following National Boards - Chiropractic, Dental, Medical, Nursing and Midwifery, Optometry, Osteopathy, Pharmacy, Physiotherapy, Podiatry and Psychology – are required to comply with the health care records section of their relevant code of conduct/guidelines/competency standards. On 1 July 2012 the following healthcare personnel will be represented by a national registration board – Aboriginal and Torres Strait Islander health practitioners, Chinese medicine practitioners, medical radiation practitioners, and occupational therapists [http://www.ahpra.gov.au/](http://www.ahpra.gov.au/).
Medical Practitioner | A person registered under the Health Practitioner Regulation National Law (NSW) in the medical profession.
---|---
Public health organisation (PHO) | a) Local health district  
b) Statutory health corporation that provides patient/client services,  
c) Affiliated health organisation in respect of its recognised establishment or recognised service that provides patient/client services, or  
d) Ambulance Service of NSW.
Should | Indicates an action that ought to be followed unless there are justifiable reasons for taking a different course of action.

1.3 Privacy and confidentiality

All information in a patient/client’s health care record is confidential and subject to prevailing privacy laws and policies. Health care records contain health information which is protected under legislation. The requirements of the legislation, including the Privacy Principles, are explained in plain English in the NSW Privacy Manual for Health Information. Health care personnel should only access a health care record and use or disclose information contained in the record when it is directly related to their duties and is essential for the fulfilment of those duties, or as provided for under relevant legislation.

1.4 Auditing

Health care records across all settings and clinical areas must be audited for compliance with this policy. PHOs must establish a framework and schedule for auditing of records and approve and designate audit tools and processes.

Clinical audits of documentation in health care records should involve a team based approach with the clinical team consisting of medical practitioners, nurses, midwives, allied health practitioners and other health care personnel, as appropriate.

Health care record audit results should be:

- a) Provided to relevant clinical areas and health care personnel.
- b) Included in PHO performance reports.
- c) Referred to PHO quality committees to facilitate quality improvement.

1.5 Education

PHOs must establish a framework for the development and delivery of suitable education on documentation and management of health care records. All health care personnel who document or manage health care records must be provided with appropriate orientation and ongoing education on the documentation and management of health care records.

The content and delivery of education programs should be informed by health care record audits. The results of such audits should be used to target problem areas relating to particular health care personnel groups or facets of documentation and management.
Specific education must be conducted for the introduction of any new complex health care record forms and for changes in documentation models.

2. DOCUMENTATION

2.1 Identification on every page/screen\(^5\)

The following items must appear on every page of the health care record, or on each screen of an electronic record (with the exception of pop up screens where the identifying details remain visible behind):

a) Unique identifier (eg. Unique Patient Identifier, Medical Record Number).
b) Patient/client’s family name and given name/s.
c) Date of birth (or gestational age/age if date of birth is estimated).
d) Sex. The exception is ObstetriX records where sex of the mother is not recorded.

2.2 Standards for documentation\(^6\)

Documentation in health care records must comply with the following:

a) Be clear and accurate.
b) Legible and in English.
c) Use approved abbreviations and symbols.
d) Written in dark ink that is readily reproducible, legible, and difficult to erase and write over for paper based records.
e) Time of entry (using a 24-hour clock – hhmm).
f) Date of entry (using ddmmyy or ddmmyyyy).
g) Signed by the author, and include their printed name and designation. In a computerised system, this will require the use of an appropriate identification system eg. electronic signature.
h) Entries by students involved in the care and treatment of a patient/client must be co-signed by the student’s supervising clinician.\(^7\)
i) Entries by different professional groups are integrated ie. there are not separate sections for each professional group.
j) Be accurate statements of clinical interactions between the patient/client and their significant others, and the health service relating to assessment; diagnosis; care planning; management/treatment/services provided and response/outcomes; professional advice sought and provided; observation/s taken and results.
k) Be sufficiently clear, structured and detailed to enable other members of the health care team to assume care of the patient/client or to provide ongoing service at any time.
l) Written in an objective way and not include demeaning or derogatory remarks.
m) Distinguish between what was observed or performed, what was reported by others as happening and/or professional opinion.
n) Made at the time of an event or as soon as possible afterwards. The time of writing must be distinguished from the time of an incident, event or observation being reported.
o) Sequential - where lines are left between entries they must be ruled across to indicate they are not left for later entries and to reflect the sequential and contemporaneous nature of all entries.

---


\(^6\) Each registered health practitioner is required to comply with the health care records section of the code of conduct/guidelines/competency standards under their relevant National Board

p) Be relevant to that patient/client.
q) Only include personal information about other people when relevant and necessary for the care and treatment of the patient client.
r) **Addendum** – if an entry omits details any additional details must be documented next to the heading ‘Addendum’, including the date and time of the omitted event and the date and time of the addendum. For hardcopy records, addendums must be appropriately integrated within the record and not documented on additional papers and/or attached to existing forms.
s) **Written in error** - all errors are must be appropriately corrected.

No alteration and correction of records is to render information in the records illegible.

An original incorrect entry must remain readable i.e. do not overwrite incorrect entries, do not use correction fluid. An accepted method of correction is to draw a line through the incorrect entry or 'strikethrough' text in electronic records; document “written in error”, followed by the author’s printed name, signature, designation and date/time of correction.

For electronic records the history of audited changes must be retained and the replacement note linked to the note flagged as “written in error”. This provides the viewer with both the erroneous record and the corrected record.

### 2.3 Documentation by medical practitioners

Documentation by medical practitioners must include the following:

a) Medical history, evidence of physical examination.
b) Diagnosis/es (as a minimum a provisional diagnosis), investigations, treatment, procedures/ interventions and progress for each treatment episode. A principal diagnosis must be reported for every episode of admitted patient care.
c) Medical management plan.
d) Where an invasive procedure is performed and/or an anaesthetic is administered, a record of the procedure including completion of all required procedural checklists. Where a general anaesthetic is administered, a record of examination by a medical practitioner prior to the procedure is also required.
e) Comprehensive completion of all patient/client care forms.
f) A copy of certificates, such as Sick and Workers Compensation Certificates, provided to patients/clients must be retained in the patient/client’s health care record.

#### 2.3.1 Attending Medical Practitioner

The Attending Medical Practitioner (AMP) is responsible for the clinical care of the patient/client for that episode of care and is responsible for ensuring that adequate standards of medical documentation are maintained for each patient/client under their care.

When documentation is delegated to a medical practitioner e.g. Intern, Resident, Registrar, the AMP remains responsible for ensuring documentation is completed to an appropriate standard that would satisfy their professional obligations.

The AMP should review the preceding medical entries and make a written entry in the health care record (print name, signature, designation and date/time) to confirm they have been read at the same time as they are reviewing the medical management plan for the patient/client to ensure it remains current and clinically appropriate, consistent with the AMP’s duty of care to the patient/client.
2.4 Documentation by nurses and midwives

Documentation by nurses and midwives must include the following:

a) Care/treatment plan, including risk assessments with associated interventions.
b) Comprehensive completion of all patient/client care forms.
c) Any significant change in the patient/client’s status with the onset of new signs and symptoms recorded.
d) If a change in the patient/client’s status has been reported to the responsible medical practitioner documentation of the name of the medical practitioner and the date and time that the change was reported to him/her.
e) Documentation of medication orders received verbally, by telephone/electronic communication including the prescriber’s name, designation and date/time.

2.5 Frequency of documentation

The frequency of documentation entries should conform to the following as minimum requirements.

2.5.1 Acute Care Patient/clients

a) Registered Nurse/Midwife, Enrolled/Endorsed Nurse should make an entry in the patient/client’s health care record a minimum of once a shift. An entry by an Assistant in Nursing should not be the only entry for a shift. Entries should reflect in a timely way the level of assessment and intervention. The results of significant diagnostic investigations and significant changes to the patient/client’s condition and/or treatment should be documented as these occur.
b) Medical practitioners should make an entry in the health care record at the time of events, or as soon as possible afterwards, including when reviewing the patient/client.
c) Other health care personnel should make entries to reflect their level of assessment and intervention consistent with the medical management plan.

2.5.2 Long Stay or Residential Patients/Clients

Depending on the health care setting and the length of stay (or expected length of stay) of the patient/client, health care personnel should make an entry at least weekly in the health care record particularly when warranted by the patient’s medical condition or frailty. Additional entries should be made to reflect changes in the patient/client status, condition and/or treatment or care plan as these occur.

2.5.3 Non-Admitted Patient/Clients

An entry must be made in the health care record for each patient/client attendance (including video conference sessions) and for failures to attend.

Entries should reflect the level of assessment and intervention. The results of significant diagnostic investigations and significant changes to the patient/client’s condition and/or treatment should be documented.

Attendance of individual patient/clients at sessions of a formal multiple session group program should be noted. Such attendances may be documented in an attendance register or scheduling system rather than the patient/client’s health care record. Where a patient/client receives specific individual care or treatment in addition to the group session interaction, this care or treatment should be documented in their health care record.

36(10/01/13)

---

2.6 Alerts and allergies

Clinicians must flag issues that require particular attention or pose a threat to the patient/client, staff or others including:

a) Allergies/sensitivities or adverse reactions, and the known consequence.

b) Infection prevention and control risks.

c) Behaviour issues that may pose a risk to themselves or others.

d) Child protection/well being matters including
   i. alerts and flags for High Risk Birth Alerts or prenatal reports
   ii. children at risk of significant harm
   iii. where NSW Police or the Department of Family and Community Services have issued a general alert to a PHO.

e) Where patients/clients have similar names and other demographic details.

PHOs must implement systems for the identification of such alerts and allergies. If a label is used on the outside folder of a paper based health care record this does not negate the need for documentation in the health care record of the alert/allergy, and known consequence.

Any such issue should be ‘flagged’ or recorded conspicuously on appropriate forms, screens or locations within the health care record. Where alerts relate to behaviour issues or child protection matters the alert should be discreet to ensure the privacy and safety of the patient/client, staff or others.

These flags, especially where codes or abbreviations are used, must be apparent to and easily understood by health care personnel; must not be ambiguous; and should be standardised within the PHO.

A flag should be reviewed at each admission. When alerts and allergies are no longer current this must be reflected in the health care record and inactivated where possible.

2.7 Labels

Non-permanent adhesive labels should be avoided. Where considered essential the label must be relevant to the patient/client and placed so that all parts of the health care record are able to be read and patient/client privacy maintained. State approved labels must be used.

2.8 Tests – requests and results

The health care record must document pathology, radiology and other tests ordered, the indication and the result.

When tests are ordered the name of the ordering medical practitioner/approved clinician and their contact number must be clearly printed (if written) or entered (if computerised) on the request form.

Pathology, radiology and other test results must be followed up and reviewed with notation as to action required. The results must be endorsed by the receiving medical practitioner/approved clinician, with endorsement involving the name, signature, designation of the medical practitioner/approved clinician, and date/time.
PHOs must develop local procedures, including steps to be taken, when:

a) Relevant details on the request form are incomplete or illegible.
b) The ordering medical practitioner/approved clinician is not on duty or contactable.

**Critical/unexpected/abnormal results** should be documented in the patient/client’s health care record by the responsible medical practitioner/approved clinician as soon as practicable and any resultant change in care/treatment plans documented.

### 2.9 Patient/client clinical incidents

All actual clinical incidents must be documented in the patient/client’s health care record. Staff must document in the health care record.

a) Incident Information Management System (IIMS) identification number.
b) Clinically relevant information about the incident.
c) Interactions related to open disclosure processes.

### 2.10 Complaints

Complaint records are not to be kept with the patient’s health care record.

### 2.11 Emergency Department records

Emergency Department records must include the following:

a) Date and time triaged including triage score.
b) Presenting problem and triage assessment.
c) Date and time seen by a medical practitioner, other clinicians such as a Clinical Initiatives Nurse, Nurse Practitioner, nursing, midwifery and allied health staff.
d) Medical, nursing, midwifery and allied health assessment.
e) Pathology, radiology and other tests ordered. Pathology, radiology and other test results must be followed up and reviewed with notation as to action required.
f) Description of critical/unexpected/abnormal pathology, radiology and other test results. If the patient/client has left the Emergency Department and not been admitted, document the steps taken to contact the patient/client or their carer if the test results indicate that urgent treatment/care is required.
g) Details of treatment.
h) Follow up treatment where applicable.
i) Transfer of care date and time, destination (eg. home, other level of health care) method and whether accompanied.

### 2.12 Anaesthetic reports

Anaesthetic reports must include the following:

a) Pre-operative assessment, including patient anaesthetic history.
b) Risk-rating eg. American Society of Anaesthesiologists (ASA) score.
c) Date and time anaesthetic commenced and completed.
d) Anaesthesia information and management ie. medications, gases, type of anaesthetic.
e) NSW safety checklists including patient assessment and equipment checklists consistent with Australian and New Zealand College of Anaesthetists requirements.
f) Operative note/monitor results.
g) Post-operative notes/orders.

---

2.13 Operation/procedure reports

Operation/procedure reports must include the following:

a) Date of operation/procedure.
b) Pre-operative and post-operative diagnosis.
c) Indication for operation/procedure.
d) Procedure safety checklist.
e) Surgical operation/procedure performed.
f) Personnel involved in performing the operation/procedure.
g) Outline of the method of surgery/procedure.
h) Product/device inserted and batch number.
i) Changes to, or deviations from, the planned operation/procedure, including any adverse events that occurred.
j) Operative/procedural findings.
k) Tissue removed.
l) Pathology ordered on specimens.
m) Post-operative orders.

2.14 Telephone/electronic consultation with patient/clients

When clinical information is provided to a patient/client, or their carer/guardian/advocate, the consultation must be documented in the health care record. The identification of the caller must be documented.

Where the caller is not the patient/client, or their carer/guardian/advocate obtain consent from the patient/client, or their carer/guardian/advocate prior to the consultation. Document the

a) Caller’s name,
b) Relationship to the patient/client, and
c) That the patient/client, or their carer/guardian/advocate has consented to the caller seeking clinical information about the patient/client in the patient/client’s health care record.

2.15 Telephone/electronic consultation between clinicians

Where a clinician involved in the care and treatment of a patient/client formally consults another clinician, via telephone/electronic means, about the patient/client and the consulted clinician provides advice, direction or action, that advice, direction or action must be documented in the health care record by the clinician seeking the advice. The name and designation of the consulted clinician, and the date/time of the consultation must also be documented as soon as practical following consultation with the other clinician and in a manner as to ensure continuity of care for patients.

2.16 Leave taken by patients/clients

Any leave taken by the patient/client should be documented in their health care record with the date/time the patient/client left and returned. The patient/client should be assessed before proceeding on leave and the outcome of that assessment documented in the health care record, together with the documented approval of the AMP noting the assessment.
2.17 Leaving against medical advice

A patient/client who decides to leave the health service/program against medical advice must be asked to sign a form to that effect with the form filed in the patient/client’s health care record. If the patient/client refuses to sign the form this must be documented in the health care record, including any advice provided.

Examples of advice that could be provided to the patient/client include:

a) The medical consequences of the patient’s decision, including the potential consequences of no treatment.

b) The provision or offering of an outpatient management plan and follow-up that is acceptable and relevant to the patient.

c) Under what circumstances the patient should return, including an assurance that they can elect to receive treatment again without any prejudice.

3. MANAGEMENT

3.1 Responsibility and accountability

The Chief Executive of the PHO must comply with the State Records Act and its regulation in respect of health care records.12

Responsibility for the maintenance of appropriate health care records must be included in the terms and conditions of appointment (including position descriptions) for all health care personnel as defined in this policy.

Documentation must be included as a standing item in annual performance reviews of clinicians. Failure to maintain adequate health care records will be managed in accordance with current NSW Health policies and guidelines for managing potential misconduct.

3.2 Individual health care record

An individual health care record with a unique identifier (eg unique patient identifier, medical record number) must be created for each patient/client who receives health care. Every live or still born baby must be allocated a unique identifier that is different to the mother.

Where multiple patient identifiers exist for the same patient/client within a PHO there must be processes established for their reconciliation and linkage, with the ability to audit those processes.

A reference notation should be placed on the health care record to identify any relevant other documents that relate to the patient’s health care. Index or patient administration systems must reference the existence of satellite/decentralised health care records that address a specific issue and that are kept separate from the principal health care record. Due to the nature of the information contained in sexual assault records these must be maintained separately from the principal health care record and be kept secure at all times; as should child protection/wellbeing and genetics records.

Staff screening and vaccination records are considered as personnel rather than health care records and must be maintained separately.

36(10/01/13)

---


3.3 Access

Health care records should be available at the point of care or service delivery. Health care records must not be removed from the campus unless prior arrangements have been made with the PHO eg. required for a home visit, required under subpoena.

Health care records are only accessible to:

a) Health care personnel currently providing care/treatment to the patient/client.

b) Staff involved in patient safety, the investigation of complaints, audit activities or research (subject to ethics committee approval, as required).

c) Staff involved in urgent public health investigations for protecting public/population health, consistent with relevant legislation.

d) Patient/client to whom the record relates, or their authorised agent, based on a case by case basis in accordance with health service release of information policies and privacy laws.

e) Other personnel/organisations/individuals in accordance with a court subpoena, statutory authority, valid search warrant, coronial summons, or other lawful order authorised by legislation, common law or NSW Health policy.

All requests for information, that is contained in a patient/client’s health care record, from a third/external party should be handled by appropriately qualified and experienced health care personnel, such as Health Information Managers, due to the sensitive nature of health care records; the special terminology used within them; and regulatory requirements around access to, and disclosure of, information.

3.4 Ownership

The health care record is the property of the PHO providing care, and not individual health care personnel or the patient/client.

Where shared care models or arrangements exist for clinicians to treat private patient/clients within PHO facilities/settings, responsibility for the management of those health care records must be included in the terms of the arrangement between the PHO and the clinician.

3.5 Retention and durability

Health care records must be maintained in a retrievable and readable state for their minimum required retention period.

Entries should not fade, be erased or deleted over time. The use of thermal papers, which fade over time, should be restricted to those clinical documents where no other suitable paper or electronic medium is available e.g. electrocardiographs, cardiotocographs.

Electronic records must be accessible over time, regardless of software or hardware changes, capable of being reproduced on paper where appropriate, and have regular adequate backups.
3.6 Storage and security

The *Health Records and Information Privacy Act 2002* establishes statutory requirements for the storage and security of health care records, which are also included in the [NSW Privacy Manual for Health Information](http://www.health.nsw.gov.au/policies/manuals/Pages/patient-matters-manual.aspx). A summary of these requirements is provided below. However, the Privacy Manual should be consulted for further detail in this area.

Personal health information, including healthcare records, must have appropriate security safeguards in place to prevent unauthorised use, disclosure, loss or other misuse. For example, all records containing personal health information should be kept in lockable storage or secure access areas when not in use.

Control over the movement of paper based health care records is important. A tracking system is required to facilitate prompt retrieval to support patient/client care and treatment and to preserve privacy.

A secure physical and electronic environment should be maintained for all data held on computer systems by the use of authorised passwords, screen savers and audit trails. If left unattended, no personal health information should be left on the screen. Screen savers and passwords should be used where possible to reduce the chance of casual observation. Consideration may be given to providing staff with different levels of access to electronic records where appropriate (i.e. full, partial or no access).

Details of the roles and responsibilities of staff, including system administrators and IT technical and support staff, concerning the protection of health care records held on electronic information systems are given in the [NSW Health Electronic Information Security Policy](http://www.health.nsw.gov.au/policies/pd/2013/PD2013_033.html).

3.7 Disposal

Health care records, both paper based and electronic, must be disposed of in a manner that will preserve the privacy and confidentiality of any information they contain.

Disposal of data records should be done in such a way as to render them unreadable and leave them in a form from which they cannot be reconstructed in whole or in part.

Paper records containing personal health information should be disposed of by shredding, pulping or burning. Where large volumes of paper are involved, specialised services for the safe disposal of confidential material should be employed.

The disposal of health care records must be documented in the PHO’s Patient Administration System and undertaken in accordance with the relevant State General Disposal Authority.

---

4. IMPLEMENTATION SELF ASSESSMENT CHECKLIST

An Implementation Self Assessment Checklist is provided to support implementation of this policy.  

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Self Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Nil</td>
</tr>
<tr>
<td></td>
<td>In development</td>
</tr>
<tr>
<td></td>
<td>Partial</td>
</tr>
<tr>
<td></td>
<td>Mature</td>
</tr>
</tbody>
</table>

A. STRATEGIC FUNDAMENTALS

PHO has documented processes to manage health care records

PHO uses an approved abbreviation list

There are resources and support to implement the Health Care Records policy and regular monitoring of progress by a responsible officer

Key performance indicators are developed to monitor and measure implementation of the Health Care Records policy in the PHO

Examples of performance measures:

1. Patient identification is on every page of the health care record or on each screen of the electronic record.

2. Handwritten entries are legible to a reader other than the author.

B. INTEGRATION INTO NORMAL BUSINESS SYSTEMS

Responsibility and accountability for documentation and management of health care records is clearly stated in position descriptions and incorporated into performance review for all relevant health care personnel.

The design, approval and implementation of health care records forms (including electronic systems) is consistent with state policies and procedures.

36(10/01/13)
C. ORGANISATIONAL IMPLEMENTATION

A schedule is in place for auditing of health care records across clinical settings. This should include both record completeness and clinical audits.

All clinical areas are audited for compliance with the Health Care Record policy according to the schedule noted above.

Results and analysis of health care record audits are provided to clinicians and managers, and are used to inform remedial quality improvement activities.

Results and analysis of health care record audits are used to inform education on clinical documentation.

There is a process for recognition of excellence in the documentation and management of health care records.

Health care records key performance indicators are monitored at ward/unit, hospital/service and PHO level and benchmarked with appropriate peers.
NOTIFICATION OF ACUTE RHEUMATIC FEVER AND RHEUMATIC HEART DISEASE – THE NSW PUBLIC HEALTH ACT 2010 (IB2015_057)

PURPOSE

This Information Bulletin provides guidance on the addition of Acute Rheumatic Fever (ARF) and Rheumatic Heart Disease (RHD) to the list of medical conditions in Schedule 1 of the NSW Public Health Act, and to the list of notifiable diseases in Schedule 2 of the Act.

Under the provisions of the Public Health Act 2010 and the Public Health Regulation 2012, doctors, hospital chief executive officers (or general managers), pathology laboratories, directors of child care centres and school principals are required to notify certain medical conditions listed on the NSW Ministry of Health website.

KEY INFORMATION

On 2 October 2015 the NSW Public Health Act 2010 was amended to add ARF and RHD in a person under the age of 35 to:

a) The list of medical conditions in Schedule 1 to that Act:
   i. That must be notified by medical practitioners to the Secretary of the NSW Ministry of Health, and

b) The list of notifiable diseases in Schedule 2 to that Act:
   i. That must be notified by health practitioners providing care in hospitals to the chief executive officer of the hospital concerned, and
   ii. That must be notified by the chief executive officer of a hospital to the Secretary of the NSW Ministry of Health.

NOTIFICATION MECHANISMS

Information on the notification of infectious diseases under the Public Health Act 2010 is detailed in the Information Bulletin IB2013_010.

Infectious disease notifications should be directed to the local Public Health Unit, and should be initiated as soon as possible within 24 hours of diagnosis.

In order to protect patient confidentiality, notifications must not be made by facsimile machine except in exceptional circumstances and when confidentiality is ensured.

Disease notification guidelines and notification forms for notifiers are available at: www.health.nsw.gov.au/Infectious/Pages/notification.aspx
PURPOSE
This guideline presents the current best evidence for conducting a youth health and wellbeing Assessment. Its purpose is to inform practice for healthcare providers to achieve the best possible care in NSW.

This guideline is primarily for clinicians caring for young people (12-24 years old) in a paediatric, adolescent or adult healthcare setting.

This guideline supports NSW Health’s commitment to implement appropriate psychosocial assessment tools, such as HEEADSSS, to assess and respond to the holistic health and wellbeing needs of young people outlined in the NSW Youth Health Framework 2017-2024 (PD2017_019).

KEY PRINCIPLES
Youth health and wellbeing assessments are important to assist clinicians to identify and respond early to areas of concern in a young person’s life that might affect their health and wellbeing.

The youth health and wellbeing assessment is not a diagnostic tool. It is a holistic, flexible approach designed to build rapport and engage with a young person in a clinical setting. The information gathered can then be used to directly address any concerns and/or refer a young person for a specialist response.

The most widely used youth health and wellbeing assessment tool in Australia and internationally is known as a HEEADSSS assessment.

Each letter of HEEADSSS reflects a major domain of a young person’s life. Capturing information in each domain helps reveal risks, behaviours and protective factors. It helps to identify areas of intervention where the clinician can work with the young person to achieve better health outcomes.

- **H** Home
- **E** Education and Employment
- **E** Eating and Exercise
- **A** Activities, Hobbies and Peer Relationships
- **D** Drug Use (cigarettes, alcohol)
- **S** Sexual Activity and Sexuality
- **S** Suicide, Self-Harm, Depression, Mood, Sleeping Patterns
- **S** Safety and Spirituality

In general, a youth health and wellbeing assessment (12-24 years old) should be conducted with every young person who attends a health service or hospital. Where appropriate young people in an adult or paediatric inpatient area within a hospital should have a youth health and wellbeing Assessment completed in conjunction with other screening assessment/admission processes.
Clinical judgement should be used to determine the appropriateness of the assessment for 12-24 year olds. This includes considering the young person’s health condition, maturity, the environment and health service context (for example, sufficient time or privacy may not be available in an Emergency Department context).

In general an assessment is done through conversation with a young person. On some occasions, where it is more appropriate a young person can be asked to complete the Youth Health and Wellbeing Assessment Chart (Appendix 1).

It is essential that clinicians/healthcare workers read and understand this guideline in particular Sections 6 to 11 of the Guideline.

- Section 6 Issues covered by a youth health and wellbeing assessment
- Section 7 When to conduct a youth health and wellbeing assessment
- Section 8 Youth health and wellbeing assessment flow diagram
- Section 9 Self-completed assessment using Youth Health and Wellbeing Assessment Chart
- Section 10 Setting up and concluding the assessment
- Section 11 Contraindications and cautions

**USE OF THE GUIDELINE**

This guideline should be considered when conducting Youth Health and Wellbeing Assessment with young people (12-24 years old) who attend a health service or hospital.

This document outlines the -

- approach that should be taken by NSW Health staff when conducting a youth health and wellbeing assessment (Sections 7 - 10)
- issues to consider when implementing the youth health and wellbeing assessment within different health settings and with different age groups (Sections 11 - 12)

A range of resources for workers are available to support Youth Health and Wellbeing Assessment when needed (Appendices 1 – 4).

The document should not be seen as a prescriptive set of rules to be applied without the clinical input and discretion of the managing health professionals. Each patient should be individually evaluated and a decision made as to appropriate management in order to achieve the best clinical outcome.

**The Youth Health and Wellbeing Assessment: Guideline is available at:**

61(01/02/18)
COVID-19 DATA COLLECTION AND REPORTING REQUIREMENTS NSW HEALTH INTRANET PAGE  (IB2020_012)

PURPOSE
Advise all NSW Health Districts and Networks of the ‘COVID-19 Data Collection and Reporting Requirements’ NSW Health intranet page.

KEY INFORMATION
Data collection and reporting, source system and business process changes must be implemented to facilitate the identification, recording and reporting of impacts of the COVID-19 pandemic on the NSW Health system.

IMPLEMENTATION
Data collection and reporting requirements relating to COVID-19 are evolving frequently in response to different and more complex information needs identified at State and Commonwealth levels.

Data collection and reporting requirement changes impacting on business processes, source systems and data collections will be published by Information Bulletin.

Advisory documents are also being regularly produced to provide advice to the NSW Health system on the management and monitoring of the COVID-19 pandemic.

A NSW Health intranet page has been established to provide a ‘one-stop shop’ for all COVID-19 related updates to core NSW Health patient focused activity data collections.

This intranet page is located at:

The intranet page will be updated as changes to data collection and reporting requirements are determined. Staff should visit the intranet page regularly to appraise themselves of the latest COVID-19 related data collection and reporting requirements for the relevant data collections.

CLARIFICATION ADVICE
The System Information and Analytics Branch, NSW Ministry of Health will provide clarification advice regarding these data collection and reporting requirements. Requests for advice should be directed to the Data Integrity and Governance Team of the System Information and Analytics Branch.

Advisory documents developed to support state-wide advice on data collection and reporting requirements to the NSW Health system may be submitted to the Data Integrity and Governance Team, System Information and Analytics Branch, NSW Ministry of Health for publishing on the NSW Health intranet page.

Contact: Patrick Fleming
Position: Data Governance Support Officer
Email: MOH-DataGovernance@health.nsw.gov.au
Telephone: 02 9391 9710
COVID-19 DATA COLLECTION SUMMARY ADVISORY (IB2020_011)

PURPOSE
To provide advice to all NSW Health services, private hospitals and day procedure centres, regarding data collection and reporting of COVID-19 (2019 novel coronavirus) for the Emergency Department, Admitted Patient and Non-Admitted Patient Data Collections.

KEY INFORMATION


62(09/04/20)

COVID-19 WARDS SET UP ADVICE (IB2020_013)

PURPOSE
To advise all NSW Health Districts and Networks about setting up new wards and repurposing existing wards for COVID-19 in the Health Entity Registration On-line (HERO), NSW Health Bed Reporting System (BRS), Patient Flow Portal and Electronic Record for Intensive Care (eRIC)

KEY INFORMATION
In response to the COVID-19 pandemic, several additional and/or re-purposed wards have been implemented across NSW Health. These must be registered in the Patient Administration System (PAS) and HERO first, then set up in the BRS, PFP, eRIC and other applicable downstream systems.


62(17/04/20)