

---

# Privacy Manual for Health Information

2025 Revision

NSW Health

NSW Ministry of Health  
1 Reserve Road  
ST LEONARDS NSW 2065  
Tel. (02) 9391 9774  
Fax. (02) 9391 9101  
TTY. (02) 9391 9900  
[www.health.nsw.gov.au](http://www.health.nsw.gov.au)

This work is copyright. It may be reproduced in whole or in part for study or training purposes subject to the inclusion of an acknowledgement of the source. It may not be reproduced for commercial usage or sale. Reproduction for purposes other than those indicated above requires written permission from the NSW Ministry of Health.

The NSW Ministry for Health acknowledges the traditional custodians of the lands across NSW. We acknowledge that we live and work on Aboriginal lands. We pay our respects to Elders past and present and to all Aboriginal people.

Further copies of this document can be downloaded from the NSW Health webpage  
[www.health.nsw.gov.au](http://www.health.nsw.gov.au)

© NSW Ministry of Health 2025

SHPN (LRS) 240064  
ISBN 978-1-76023-784-4

February 2025

# Contents

<b>1</b>	<b>Definitions and acronyms.....</b>	<b>5</b>	<b>4.3</b>	<b>Common law, professional and other obligations to protect privacy.....</b>	<b>18</b>
<b>2</b>	<b>Executive summary .....</b>	<b>9</b>	4.3.1	Duties of confidentiality.....	18
2.1	Overview of privacy legislation.....	9	4.3.2	NSW Health Code of Conduct.....	18
2.2	Summary of the Health Privacy Principles (or HPPs).....	10	4.3.3	Registered health professionals.....	19
2.3	Quick reference to structure of the Manual.....	11	4.3.4	Disciplinary matters and ICAC reporting.....	19
<b>3</b>	<b>Scope .....</b>	<b>12</b>	<b>5</b>	<b>Key concepts .....</b>	<b>20</b>
3.1	Who is bound by the Manual?.....	12	5.1	Health information .....	20
3.2	NSW Health agencies to be treated as a single agency.....	12	5.2	Personal information.....	20
3.3	What sort of information does the Manual cover?.....	13	5.3	De-identified information.....	21
3.4	What is not covered?.....	13	5.4	Consent.....	22
3.5	What our patients have a right to expect.....	13	5.4.1	Elements of consent.....	22
3.6	What health staff and service providers have a right to expect .....	13	5.4.2	Implied consent .....	22
3.7	What other NSW Health resources should be considered.....	14	5.4.3	Express consent.....	22
3.8	Privacy Framework for NSW Health staff.....	14	5.4.4	Deciding if consent is needed.....	23
<b>4</b>	<b>Other obligations .....</b>	<b>15</b>	5.5	Test for capacity.....	23
4.1	Privacy laws and related legislation .....	15	5.5.1	General rule.....	23
4.1.1	General secrecy provisions.....	15	5.5.2	Minors .....	24
4.1.2	Mental health.....	15	5.6	Authorised representative .....	24
4.1.3	Serious adverse event reviews.....	16	5.6.1	Definition of an ‘authorised representative’ .....	24
4.1.4	Epidemiological information.....	16	5.7	‘Reasonable’ and ‘practicable’ .....	26
4.1.5	HIV/AIDS-related information.....	16	5.8	‘Sensitive’ information and patient expectations .....	25
4.1.6	Children and Young Persons (Care and Protection) Act 1998 (NSW) .....	16	5.8.1	Specific health services.....	26
4.1.7	Crimes (Domestic and Personal Violence) Act 2007.....	16	5.8.2	Patient requests.....	27
4.1.8	Privacy Act 1988 (Cth) .....	16	5.8.3	Non-personal ‘sensitive’ information.....	27
4.1.9	Mandatory reporting under Commonwealth legislation.....	17	<b>6</b>	<b>Responsibilities under privacy law .....</b>	<b>28</b>
4.1.10	My Health Records Act 2012 (Cth).....	17	6.1	Chief Executives.....	28
4.1.11	National Disability Insurance Scheme Act 2013 (Cth) .....	17	6.1.1	Key obligations .....	28
4.2	Other laws regulating information management.....	18	6.1.2	Staff training.....	28
4.2.1	State Records Act 1998 (NSW).....	18	6.1.3	Mandatory training .....	29
4.2.2	Government Information (Public Access) Act 2009 (NSW) (GIPA Act).....	18	6.1.4	Staff communication and alerts.....	29
			6.2	Privacy Contact Officer.....	29
			6.3	Other staff .....	30
			6.3.1	Managers and supervisors .....	30
			6.3.2	Health care providers.....	31
			6.3.3	Funding and grants administrators.....	31
			6.3.4	Information systems and information technology (IT) managers.....	31
			6.4	Contracted agencies .....	31
			6.5	Compliance tips.....	32

6.6	NSW Health privacy webpage and key privacy resources.....	32	11	Using and disclosing personal health information (HPPs 10 & 11) .....	50
6.7	Privacy annual reporting .....	32	11.1	Use and disclosure for the 'primary purpose' .....	50
7	Collecting personal health information (HPPs 1 – 4) .....	33	11.2	Use and disclosure for a 'secondary purpose' .....	51
7.1	When can you collect information? (HPP 1) .....	33	11.2.1	Directly related purpose HPP 10(1)(b) & 11(1)(b).....	51
7.2	How should information be collected? (HPP 2).....	33	11.2.2	Consent.....	52
7.3	Who should information be collected from? (HPP 3).....	34	11.2.3	Uses and disclosures regarding threats to health and safety, and public health HPP 10&11(1)(c).....	55
7.4	Informing individuals about what is collected (HPP 4).....	34	11.2.4	To assist in a 'stage of emergency' .....	57
7.4.1	Who do you need to inform if you have collected the information?.....	34	11.2.5	Management, training or research HPPs 10 & 11 (1) (d), (e) & (f).....	58
7.4.2	What information do individuals need to be told? .....	35	11.2.6	Finding a missing person.....	60
7.4.3	When should individuals be told? .....	35	11.2.7	Investigating and reporting wrong conduct.....	60
7.4.4	How should individuals be told?.....	35	11.2.8	Law enforcement agencies, including police .....	60
7.4.5	Privacy Leaflet for Patients.....	36	11.2.9	Investigative agencies.....	63
7.4.6	Privacy poster.....	37	11.2.10	Disclosure on compassionate grounds .....	64
7.4.7	Youth-friendly privacy resources.....	37	11.2.11	Chaplaincy services .....	65
8	Anonymity (HPP 13) .....	38	11.3	Use and disclosure authorised by law – HPPs 10(2) and 11(2) .....	87
8.1	When providing a service anonymously may be impracticable.....	38	11.3.1	NSW Ministry of Health Officers and Environmental Health Officers.....	66
8.2	When providing a service anonymously may be unlawful.....	38	11.3.2	Child protection.....	66
8.3	Use of alias or 'disguised identity' .....	38	11.3.3	Disclosing health information of custodial patients .....	69
9	Retention, security and protection (HPP 5) .....	40	11.3.4	Reporting 'serious criminal offences' and 'child abuse offences' .....	69
9.1	Retention and disposal of personal health information .....	40	11.3.5	Crimes (Domestic and Personal Violence) Act 2007 .....	70
9.2	Security of personal health information .....	41	11.3.6	Coroner .....	70
9.2.1	Hard copy health records.....	41	11.3.7	Search warrants and subpoenas.....	71
9.2.2	Images and photography.....	41	11.3.8	Health Care Complaints Commission .....	72
9.2.3	Computer systems and applications.....	42	11.3.9	The Ombudsman.....	72
9.2.4	Safeguards when delivering and transmitting information .....	44	11.3.10	Official visitors .....	72
9.2.5	Printing and copying.....	47	11.3.11	Domestic Violence Death Review Team & Child Death Review Team .....	72
9.2.6	Training and presentations.....	47	11.3.12	SafeWork NSW .....	72
9.2.7	Conversations.....	48	11.3.13	NSW Ageing and Disability Commission.....	72
9.2.8	Visibility of computer screens.....	48	11.3.14	Commonwealth Agencies .....	72
9.2.9	Whiteboards and patient journey boards in public view .....	48	11.3.15	Statutory reporting requirements .....	73
10	Accuracy (HPP 9) .....	49	11.3.16	Information required by the Minister or Premier.....	74
			11.4	Computer systems and applications.....	74

<b>12 Patient access and amendment (HPPs 6, 7 &amp; 8) .....</b>	<b>75</b>	<b>15.2 Requests from state and federal police .....</b>	<b>88</b>
12.1 Access to personal health information (HPPs 6 & 7) .....	75	15.2.1 Where disclosure to police is authorised by patient .....	88
12.2 Interaction of HRIP Act and the GIPA Act .....	75	15.2.2 Where access is not authorised by patient ....	88
12.3 Where access is refused .....	76	15.2.3 Search warrant .....	88
12.3.1 Reasons for refusing access under the GIPA Act .....	76	15.2.4 Police interviews .....	88
12.4 Providing access .....	78	<b>15.3 Violence, abuse and neglect .....</b>	<b>88</b>
12.5 Other conditions of access .....	79	15.3.1 Child Protection Counselling Records .....	89
12.5.1 Parenting orders .....	79	15.3.2 Sexual Assault Services and integrated Violence, Abuse and Neglect services .....	89
12.5.2 Apprehended Violence Order .....	79	<b>15.4 Health examinations of school children .....</b>	<b>90</b>
12.5.3 Reports to the Department of Communities and Justice (DCJ) .....	79	<b>15.5 Use of interpreters .....</b>	<b>90</b>
12.5.4 Access by staff responding to a complaint, claim or investigation .....	79	<b>15.6 Legal claims and insurance .....</b>	<b>90</b>
12.6 Obtain proof of identity .....	80	15.6.1 Claims manager and Treasury Managed Fund .....	90
12.7 Fees and charges .....	80	15.6.2 Patient's legal representative .....	90
12.8 Additions, corrections and addendums (HPP 8) .....	81	15.6.3 Patient's insurer .....	91
12.8.1 Where an alteration is included .....	81	15.6.4 NSW Motor Accident (Compulsory Third Party 'CTP') Claims .....	91
12.8.2 Where an alteration is refused .....	81	<b>15.7 Enquiries about hospital patients, including media .....</b>	<b>91</b>
<b>13 Miscellaneous (HPPs 12, 14 &amp; 15) .....</b>	<b>82</b>	15.7.1 Enquiries about patients .....	91
13.1 Identifiers (HPP 12) .....	82	15.7.2 Other safeguards for enquiries sections .....	91
13.2 Transferring personal health information out of NSW (HPP14) .....	82	15.7.3 Media queries .....	91
13.2.1 Within Australia .....	82	<b>15.8 Fundraising .....</b>	<b>92</b>
13.3 Linkage of health records (HPP 15) .....	83	15.8.1 Consent for uses or disclosures for fundraising or publicity purposes .....	92
<b>14 Complaints handling and responding to breaches .....</b>	<b>84</b>	15.8.2 Use of mailing lists .....	92
14.1 General complaint handling principles .....	84	15.8.3 Organisations with a commercial interest .....	93
14.2 Privacy internal reviews .....	84	<b>15.9 Information-specific laws and policies .....</b>	<b>93</b>
14.3 NSW Civil and Administrative Tribunal (NCAT) .....	85	15.9.1 Aboriginal health information .....	93
14.4 Responding to data breaches .....	85	15.9.2 Adoption information .....	93
14.5 Breach of privacy by an employee .....	86	15.9.3 Service-based policies .....	93
<b>15 Common privacy issues .....</b>	<b>87</b>	15.9.4 Service-based practices .....	94
15.1 Third party health care providers .....	87	15.9.5 Organ and tissue donor information .....	94
15.1.1 Informing patients .....	87	15.9.6 Managing public health risks .....	95
15.1.2 Health practitioner obligations .....	87	<b>15.10 Deceased patients .....</b>	<b>96</b>
15.1.3 Addressing patient concerns .....	87	<b>15.11 Virtual Care (Telehealth) .....</b>	<b>96</b>
15.1.4 Conclusion of care .....	87	<b>15.11A Recording online meetings involving patient health information .....</b>	<b>96</b>
15.1.5 Discharge referrals to GPs and others .....	87	<b>15.12 Community health records .....</b>	<b>97</b>
15.1.6 Records of a patient's family members .....	88	15.12.1 Group houses/hostels .....	97
		15.12.2 Group sessions .....	97
		15.12.3 Family consultations .....	97

<b>15.13 Maintaining the health record.....</b>	<b>98</b>	<b>16 Electronic health information management systems.....</b>	<b>103</b>
15.13.1 Quality of health records.....	98	<b>16.1 Electronic health records.....</b>	<b>132</b>
15.13.2 Accuracy and completeness.....	98	<b>16.2 Data collections and data warehousing.....</b>	<b>103</b>
15.13.3 Control of health records.....	98	16.2.1 Identified and de-identified data .....	104
15.13.4 Removal.....	99	<b>16.3 Fundamental principles.....</b>	<b>104</b>
15.13.5 Transfer.....	99	16.3.1 Privacy and confidentiality undertakings for staff .....	104
15.13.6 Storage, archiving and disposal .....	99	16.3.2 Training and informing staff .....	104
15.13.7 Health facility closures .....	100	16.3.3 Access protocols.....	105
<b>15.14 NSW data collections.....</b>	<b>100</b>	16.3.4 Auditing .....	105
15.14.1 NSW Health data .....	100	16.3.5 Informing patients.....	106
15.14.2 Health Information Resources Directory (HIRD).....	100	<b>16.4 Evidence Act 1995.....</b>	<b>106</b>
15.14.3 Staff roles.....	100	<b>16.5 Accountability .....</b>	<b>106</b>
15.14.4 Access to data collections.....	100	<b>16.6 Access and quality control .....</b>	<b>105</b>
15.15 Artificial Intelligence (AI) and Privacy.....	102	<b>16.7 Patient access.....</b>	<b>107</b>
		<b>16.8 My Health Record.....</b>	<b>107</b>
		16.8.1 Mandatory security and access requirements.....	107
		<b>Index .....</b>	<b>108</b>

# 1 Definitions and acronyms

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

**Accredited chaplain:** A person accredited in accordance with the [NSW Health & Civil Chaplaincies Advisory Committee NSW Memorandum of Understanding \(MOU\)](#), to provide pastoral care and chaplaincy services to patients. See **Section 11.2.11 Chaplaincy services**.

**Affiliated health organisation:** An organisation within the meaning of section 62 of the [Health Services Act 1997](#). See **Section 3.1 Who is bound by the Manual?**

**Ambulance Service of NSW:** NSW Health Service who are employed primarily in connection with the provision of ambulance services as per section 67A of the [Health Services Act 1997](#). See also 'Health service' and 'Public health system'.

**Authorised representative:** See **Section 5.6 Authorised representative**.

**Capacity:** See **Section 5.5 Test for capacity**.

**Chief Executive:** The chief executive or head of the organisation (however described). Under the [Health Services Act 1997](#), Chief Executive means the Chief Executive of a Local Health District, Specialty Network or statutory health corporation, or the person responsible to the governing body of an affiliated health organisation for management of its recognised establishments and services. For units of the Health Administration Corporation, the Chief Executive is the head of the unit.

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

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

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

**Cth:** Commonwealth

**Data breach:** Unauthorised access to, and/or the unauthorised use, disclosure or loss of information, including personal information or health information.

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

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

**Emergency:** Under HPPs 10 and 11, exemptions apply to handling of personal information in a 'stage of emergency' (prevention, preparation, response and recovery). An 'emergency' is defined by the [State Emergency and Rescue Management Act 1989 \(NSW\)](#) to mean an emergency due to an actual or imminent occurrence (such as fire, flood, storm, earthquake, explosion, terrorist act, accident, epidemic, or warlike action) which—

- (a) endangers, or threatens to endanger, the safety or health of persons or animals in the State, or
- (b) destroys or damages, or threatens to destroy or damage, property in the State, or
- (c) causes a failure of, or a significant disruption to, an essential service.

being an emergency, which requires a significant and coordinated response.

See **Section 11.2.4 To assist in a 'stage of emergency'**.

**Enduring power of attorney:** Formal document which authorises another person to make financial and legal decisions for a patient, which continues to have legal effect if the patient is unable to make these decisions for themselves during their lifetime. See also 'power of attorney,' and **Section 5.6 Authorised representative**.

**Enduring guardian:** A formal document which authorises another person to make health and lifestyle decisions on the patient's behalf, including the authority to consent to medical and dental



treatment. See **Section 5.6 Authorised representative**.

**DCJ:** The [NSW Department of Communities and Justice](#).

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

**GIPA Act:** The [Government Information \(Public Access\) Act 2009 \(NSW\)](#).

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

**Health information:** See **Section 5.1 Health information**.

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

**Note:** 'Medical Record Department', 'Health Information and Record Service', 'Clinical Information Department' are names given to the Health Information Services within NSW Health.

**Health practitioner:** Anyone, including a medical practitioner, who is a registered health professional under the [Health Practitioner Regulation National Law \(2009\)](#).

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

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

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

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

**Health service staff:** Anyone who carries out work for a NSW health service, including employees, visiting health practitioners, contractors and sub-

contractors, agency staff, volunteers, apprentices, trainees, and students. See **Section 3.1 Who is bound by the Manual?**

**Hospital:** means a hospital as defined in the [Health Services Act 1997](#), being an institution at which relief is given to sick or injured people through the provision of care or treatment.

**HPPs:** The [Health Privacy Principles](#) established under the [Health Records and Information Privacy Act 2002 \(NSW\)](#). There are 15 HPPs. See **Section 2.1 Overview of privacy legislation**.

**HREC:** [Human Research Ethics Committee](#); a committee, constituted in accordance with NHMRC guidelines, which protects the subjects of research and ensures that ethical standards are maintained by reviewing and advising on the ethical acceptability of research proposals.

**HRIP Act:** the [Health Records and Information Privacy Act 2002 \(NSW\)](#).

**HRIP Regulation:** the [Health Records and Information Privacy Regulation 2022](#) (or any regulation that updates this regulation)

See **Section 3.2 NSW Health agencies to be treated as a single agency**, **Section 11.2.11 hospital chaplains**, **Section 15.9.5 organ donor registers** and **Section 16.8 My Health Record**.

**Immediate family member:** Defined under **section 4** of the [Health Records and Information Privacy Act 2002](#) to be a person who is:

- a parent, child, or sibling of the individual, or
- a spouse of the individual (including a de facto spouse), or
- a member of the individual's household who is a relative of the individual, or
- a person nominated to an organisation by the individual as a person to whom health information relating to the individual may be disclosed.

**Local Health District (District):** A health service listed in the [Health Services Act 1997](#), Schedule 1.

**Mandatory data breach reporting:** Mandatory requirements to report HRIP Act and PPIP Act data breaches which may cause serious harm apply under the Mandatory Notification of Data Breach (MNDB) scheme. The [Privacy Act 1988 \(Cth\)](#) (the Privacy Act) and the [My Health Record Act 2012 \(Cth\)](#) also impose mandatory requirements to report data breaches in some instances. See **Section 14.4 Responding to data breaches**.



**Medical practitioner:** A registered medical professional under the [Health Practitioner Regulation National Law \(2009\)](#).

**Medical record:** See health record.

**Ministry of Health:** The NSW Ministry of Health as established under the [Government Sector Employment Act 2013](#).

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

**My Health Record:** Patient controlled electronic health record, operated as a national system by the Australian Digital Health Agency. See **Section 16 .8 My Health Record**.

**NHMRC:** [National Health & Medical Research Council](#).

**NGO:** Non-Government Organisation.

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

**NSW PHSREC:** NSW Population and Health Services Research Ethics Committee, which is the [NSW Health Human Research Ethics Committee](#) established in accordance with NHMRC guidelines.

**Parental responsibility:** Defined in section 8 of the [Health Records and Information Privacy Act 2002](#) to be all the duties, powers, responsibility, and authority which, by law, parents have in relation to their children.

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

**PCO:** Privacy Contact Officer – See **Section 6.2 Privacy Contact Officer**.

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

**Personal information:** See **Section 5.2 Personal information**.

**PIIP Act:** The [Privacy and Personal Information Protection Act 1998 \(NSW\)](#).

**Power of attorney:** A formal document in which a person of sound mind authorises a second person to

act on their behalf. See also ‘**Enduring power of attorney**,’ and **Section 5.6 Authorised representative**.

**Primary purpose:** The dominant purpose for which personal health information is collected. Most often in the health system, the primary purpose for collecting health information will be to provide care, or an episode of care.

**Privacy:** For the purposes of this Manual, ‘privacy’ refers to the right of an individual to have their personal health information safeguarded from loss, misuse, and unauthorised disclosure. See also **Section 2.1 Overview of privacy legislation**.

**Privacy breach:** Refers to any conduct that breaches any of the Information Protection Principles or the Health Privacy Principles (HPPs) (or other relevant privacy legislation) and may also refer to a **data breach** related to personal and/or health information. See **Section 14**.

**Privacy Code of Practice and Health Privacy Code of Practice:** A privacy code of practice is a legal instrument which allows a public sector agency or organisation to make changes to an Information Protection Principle (IPP) or a Health Privacy Principle (HPP). A Privacy Code of Practice may also contain provisions that deal with public registers, specifying how certain rules will apply in a particular situation. For more information, see [Information and Privacy Commission, Privacy Codes of Practice](#).

**Privacy Impact Assessment:** A Privacy Impact Assessment (PIA) is a systematic analysis which assists organisations to identify and minimise the privacy risks of new projects or changes to services. For more information, see NSW [Information and Privacy Commission, ‘Guide to Privacy Impact Assessments in NSW’](#).

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

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

**Public Interest Directions and Health Public Interest Directions:** The NSW Privacy Commissioner, with the approval of the Attorney General, may make a Public Interest Direction (Direction) to waive or

make changes to the requirements for a public sector agency to comply with an Information Protection Principle (IPP) or in consultation with the Attorney General and approval from the Minister for Health, a Health Privacy Principle (HPP). Agencies may approach the Privacy Commissioner to request a Direction, or the Privacy Commissioner may recognise a need for a Direction without a request. The general intent is for the Directions to apply temporarily. If a longer-term waiver or change in the application of an IPP is required, then a [Code of Practice](#) may be more appropriate. For more information, see [Information and Privacy Commission, 'Public Interest Directions'](#).

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

**Secondary purpose:** A purpose other than the purpose (the primary purpose) for which information was collected. The health service may use or disclose personal health information for a 'secondary purpose' in accordance with Health Privacy Principles 10 and 11. See **Section 11.2 Use and disclosure for a 'secondary purpose'**.

**Specialty Network:** Sydney Children's Hospitals Network and Justice Health and Forensic Mental Health Network.

**Staff:** See 'Health service staff'.

**Stage of emergency:** See **Section 11.2.4 State Emergency and Rescue Management Act 1989 provisions** – Under the *State Emergency and Rescue Management Act*, there are four stages of emergencies: prevention, preparation, response and recovery.

**Statutory guidelines:** Refers to guidelines under the [Health Records and Information Privacy Act 2002](#) issued by the NSW Privacy Commissioner, Information and Privacy Commission NSW. See **Section 11.2.5 Management, training, or research**.

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

**Third party information:** A patient record, personnel record or other government record may contain

personal or health information or other confidential information that relates to a third person. The redaction of information about a third party needs to be considered in any request to access or release the information.

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

**Young person:** A young person means a person who is aged 16 years or above but who is under the age of 18 years, [Children and Young Persons \(Care and Protection\) Act 1998](#), section 3. See also 'Child' and 'Minor' and **Section 5.5**.

## 2 Executive summary

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

This edition of the Privacy Manual for Health Information incorporates changes in legislation which impact on the management of personal health information, notably:

### NSW legislation

- [Health Administration Regulation 2020](#)
- [Health Records and Information Privacy Act 2002](#)
- [Health Records and Information Privacy Regulation 2022](#)
- [Mandatory Disease Testing Act 2021](#)
- [Public Health Act 2010](#)
- [Privacy and Personal Information Protection Act 1998](#)

### Commonwealth legislation

- [My Health Records Act 2012](#)

Consultation on this edition has extended to:

- the Ministry of Health
- Local Health Districts, Specialty Networks, and public health organisations (PHOs) comprising NSW Health

### 2.1 Overview of privacy legislation

Privacy in Australia has moved from a policy-based system to one regulated by law. In NSW, these laws are the [Health Records and Information Privacy Act 2002](#) which regulates health privacy, and the [Privacy and Personal Information Protection Act 1998](#) which generally applies to non-health personal information.

The role of this Manual is to provide operational guidance on compliance with the [Health Records and Information Privacy Act 2002](#).

The Health Privacy Principles (HPPs) contained in the [Health Records and Information Privacy Act 2002](#) establish rules for the management of health information. These rules are relevant in a wide range of activities of health services including staff interactions with patients, establishing and maintaining data collections and patient information systems, and the day-to-day sharing of health information for management, evaluation, training, research and other authorised purposes.


The Manual outlines procedures to support compliance including:

- ensuring personal health information is collected, stored, and used in accordance with the HPPs
- providing staff with practical tips for compliance with the HPPs
- acknowledging the responsibility of the NSW public health system to ensure that the privacy of patient information is protected
- clear guidance to provide certainty for staff involved in the day-to-day administration of patient information
- providing best practice solutions to address privacy risks associated with technological advances in the health sector including developments in virtual care and telehealth
- providing a benchmark which can be used for auditing performance.

## 2.2 Summary of the Health Privacy Principles (or HPPs)

The 15 Health Privacy Principles (or HPPs) are set out in the *Health Records and Information Privacy Act, Schedule 1*. The HPPs are summarised below for quick reference.

COLLECTION PRINCIPLES	
HPP 1	<b>Purposes of collection of personal health information</b>
Personal health information must be collected by lawful means and for a lawful purpose. The purpose must be directly related to, and reasonably necessary for, an organisation's functions or activities.	
HPP 2	<b>Collection and information sought must be relevant, not excessive, accurate and not intrusive</b>
HPP 3	<b>Collection from individual concerned</b>
Personal health information must be collected from the individual it relates to unless that is unreasonable or impractical.	
HPP 4	<b>Individual to be made aware of certain matters</b>
Reasonable steps must be taken to inform the individual about how the information may be used, who may access it, and the consequences of not providing it.	
The individual should be told what agency is collecting the information and that they have a right to access it. This information should generally also be given to the individual where information about them is collected from someone else, unless certain exemptions, listed in the Act and the guidelines apply.	
SECURITY PRINCIPLES	
HPP 5	<b>Retention and security</b>
Personal health information held by public health agencies must be securely housed and protected against loss or misuse. Information must be kept only as long as is necessary for the purpose (or as required by a law, such as the <i>NSW State Records Act 1998</i> , and must be disposed of securely.	
ACCESS AND AMENDMENT PRINCIPLES	
HPP 6	<b>Information about personal health information held by organisations</b>
Organisations that hold personal health information must allow individuals to find out if they hold information about that individual, and, if so, what kind of information they hold, what it is used for, and whether and how the individual can access it.	
HPP 7	<b>Access to personal health information</b>
Individuals must be allowed to access the personal health information held about them. This must be done without excessive expense or delay.	
HPP 8	<b>Amendment of personal health information</b>
Individuals may request that their personal health information be amended to ensure that it is accurate, relevant, up to date, complete and not misleading.	
Organisations must either make the requested amendments or, if requested, attach to the information a statement by the individual of the amendment they sought.	
ACCURACY PRINCIPLES	
HPP 9	<b>Accuracy</b>
Before using personal health information, organisations must take reasonable steps to ensure that the personal health information they hold is relevant, up to date, complete and not misleading.	
USE PRINCIPLES	
HPP 10	<b>Limits on use of personal health information</b>
Personal health information can be used for the purpose for which it was collected, or for other purposes recognised by the Act. These include a 'secondary purpose' such as where there is consent for the use, the use is a 'directly related purpose,' for management, training, and research activities, for investigation and law enforcement, or where there are serious threats to individuals or the public, or emergencies.	
DISCLOSURE PRINCIPLES	
HPP 11	<b>Limits on disclosure of personal health information</b>
The provisions for disclosure of personal health information are the same as those for use of this information.	
They also include a provision that a person's personal health information may be disclosed to immediate family members for compassionate reasons, provided that this is not contrary to the expressed wish of the individual.	

OTHER PRINCIPLES	
<b>HPP 12</b>	<b>Identifiers</b>
<p>Identifiers can only be applied to personal health information if this is reasonably necessary to carry out the organisation's functions.</p> <p>Public health system identifiers may be used by private sector agencies, but only in defined circumstances and with strict controls.</p>	
<b>HPP 13</b>	<b>Anonymity</b>
<p>Provided that it is lawful and practicable, individuals should be given the option of not identifying themselves when dealing with health organisations.</p>	
<b>HPP 14</b>	<b>Transborder data flows and data flows to Commonwealth agencies</b>
<p>As a general principle, personal health information must not be transferred to a Commonwealth agency or an organisation in another state jurisdiction unless the receiving agency applies personal health information privacy policies and procedures substantially similar to those of NSW.</p>	
<b>HPP 15</b>	<b>Linkage of health records</b>
<p>Personal health information must not be included in a system that links health records of a health service with health records in another health service outside of NSW Health, unless the individual it relates to has expressly consented.</p> <p>HPP 15 only applies to linkages of an ongoing record of health care for an individual and does not restrict linkage of other personal health information held electronically.</p> <p>HPP 15 applies to the linkage of records of health care at a state or national level between the public and private sectors, or between two or more private health services.</p>	
 <p><b>Further guidance:</b></p> <p>Section 13.3 Linkage of health records (HPP 15)</p> <p>Section 16.8 My Health Record</p>	

## 2.3 Quick reference to structure of the Manual

For a general overview of the rationale for and purpose of this Manual	Go to Section 2.1
For a summary of the Health Privacy Principles (HPPs) under the <u><a href="#">Health Records and Information Privacy Act 2002</a></u>	Go to Section 2.2
For explanation of how other laws relate to privacy law	Go to Section 4
To check the meaning of some of the key concepts used in privacy law	Go to Section 5
For a detailed explanation of the HPPs	Go to Sections 7-13
If you have received a complaint, need to conduct an internal review or respond to a data breach	Go to Section 14
For guidance on managing a privacy breach or data breach	Go to Section 14
If you need to check how to deal with common privacy issues arising in health care	Go to Section 15

If you have any feedback on the Manual, it should be sent to:

Legal and Regulatory Services  
NSW Ministry of Health  
LMB 2030, ST LEONARDS NSW 1590  
E-mail: [MOH-privacy@health.nsw.gov.au](mailto:MOH-privacy@health.nsw.gov.au)

# 3 Scope

## 3.1 Who is bound by the Manual?

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

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

Persons to whom the Manual applies include:

- providers of health services such as doctors, nurses, midwives, case managers, visiting providers and allied health staff
- administrators, clerical, and service staff
- technical, scientific and laboratory personnel
- auditors
- interpreters
- accredited chaplains
- pastoral care workers
- volunteers
- students
- consultants
- temporary and contract staff
- external custodians of health information owned by NSW Health, e.g. contractors engaged for physical or electronic warehousing of medical records or for other purposes.

The Manual applies to NSW Health, which covers:

- Local Health Districts (Districts)
- Statutory Health Corporations
- Specialty Networks
- Affiliated health organisations
- Units of the Health Administration Corporation, including the Ambulance Service of NSW
- NSW Ministry of Health
- Cancer Institute NSW
- Health Professional Councils Authority

- any other health service provided by the public health system including nursing homes, hostels and group homes, community health services, drug and alcohol services, allied health programs, dental and early childhood services, multi-purpose services, scientific and laboratory services and health promotion and public health services
- non-government organisations, where compliance is required by their Funding Agreement with NSW Health.



### Further guidance:

- [Corporate Governance & Accountability Compendium for NSW Health](#)
- [Privacy Leaflet for Staff](#)

## 3.2 NSW Health agencies to be treated as a single agency

In accordance with clause 10 of the [Health Records and Information Privacy Regulation 2022](#), the following health agencies are to be treated as a single agency for the purposes of the Health Privacy Principles and any health privacy codes of practice:

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

This Regulation enables multiple NSW Health agencies to provide health services to an individual within the scope of the 15 Health Privacy Principles.

Use of personal health information between these agencies must still comply with the requirements of HPP 10 (Limits on use). Personal health information can only be used for the purpose it was collected or for a directly related purpose which the patient/individual would reasonably expect (unless there is another lawfully authorised exception).



### Further guidance:

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



### 3.3 What sort of information does the Manual cover?

The Manual covers personal health information. Under the [Health Records and Information Privacy Act 2002](#) this means personal information that is identifying information, or which could reasonably link to identifying information, collected from or about individual people in order to provide them with health services. See Sections 5.1 Health information, and 5.2 Personal information.

Both the [Health Records and Information Privacy Act 2002](#) and the Manual cover all types of dealings with personal health information, including collection, storage, security, use, disclosure, access, transfer, and linkage of health records. They apply to personal health information in any format, including electronic and online formats as well as paper-based health records. While different formats will require different approaches and procedures, the underlying principles remain the same.

### 3.4 What is not covered?

The [Health Records and Information Privacy Act 2002](#) and the Manual do NOT apply to:

- information that is not 'personal information', but which may be considered sensitive such as tender documents, private hospital licensing information or Cabinet documents (the confidentiality of these types of information may be required by the [State Records Act 1998](#) and, in some circumstances, the [Government Information \(Public Access\) Act 2009 \(NSW\)](#) (GIPA Act)).
- information that is not personal information because it is 'de-identified' and not re-identifiable, or because the identity of a person is not reasonably ascertainable from the information. For guidance on what constitutes 'de-identified' information see Section 5.3 De-identified information.
- personal information which is not health information, such as payroll records or personnel files which are regulated by the [Privacy and Personal Information Protection Act 1998](#) and are addressed by the [NSW Health Privacy Management Plan](#).
- personal information and health information which is already on the public record.
- statistical or other aggregated information.



#### Further guidance:

- [NSW Health Privacy Management Plan](#)
- [NSW Health Code of Conduct \(PD2015\\_049\)](#)

### 3.5 What our patients have a right to expect

Patients should be informed of the following:

- their personal health information will be protected in accordance with the [Health Records and Information Privacy Act 2002](#)
- their personal health information will only be given to another person if it is important for their health care or can be otherwise legally justified
- they are, subject to limited exceptions, entitled to access their own health records and have those records amended to correct inaccuracies
- provided it is both legal and practicable to do so, they have the option to obtain services anonymously, see Section 8 Anonymity (HPP 13)
- comprehensive clinical information will be available to their health care providers to enable optimal care
- the process for making privacy complaints or raising concerns about the handling of their health information.



#### Further guidance:

- Section 7 – Collecting personal health information (HPPs 1-4)
- [NSW Health Privacy Management Plan](#)
- [NSW Health Privacy Leaflet for Patients](#)

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

NSW Health is committed to ensuring that information which supports the provision of health care is readily available to authorised users, when and where it is needed and is delivered in a timely and efficient manner. Accordingly, the Manual supports the principles in the [Health Records and Information Privacy Act 2002](#) which also promote:

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

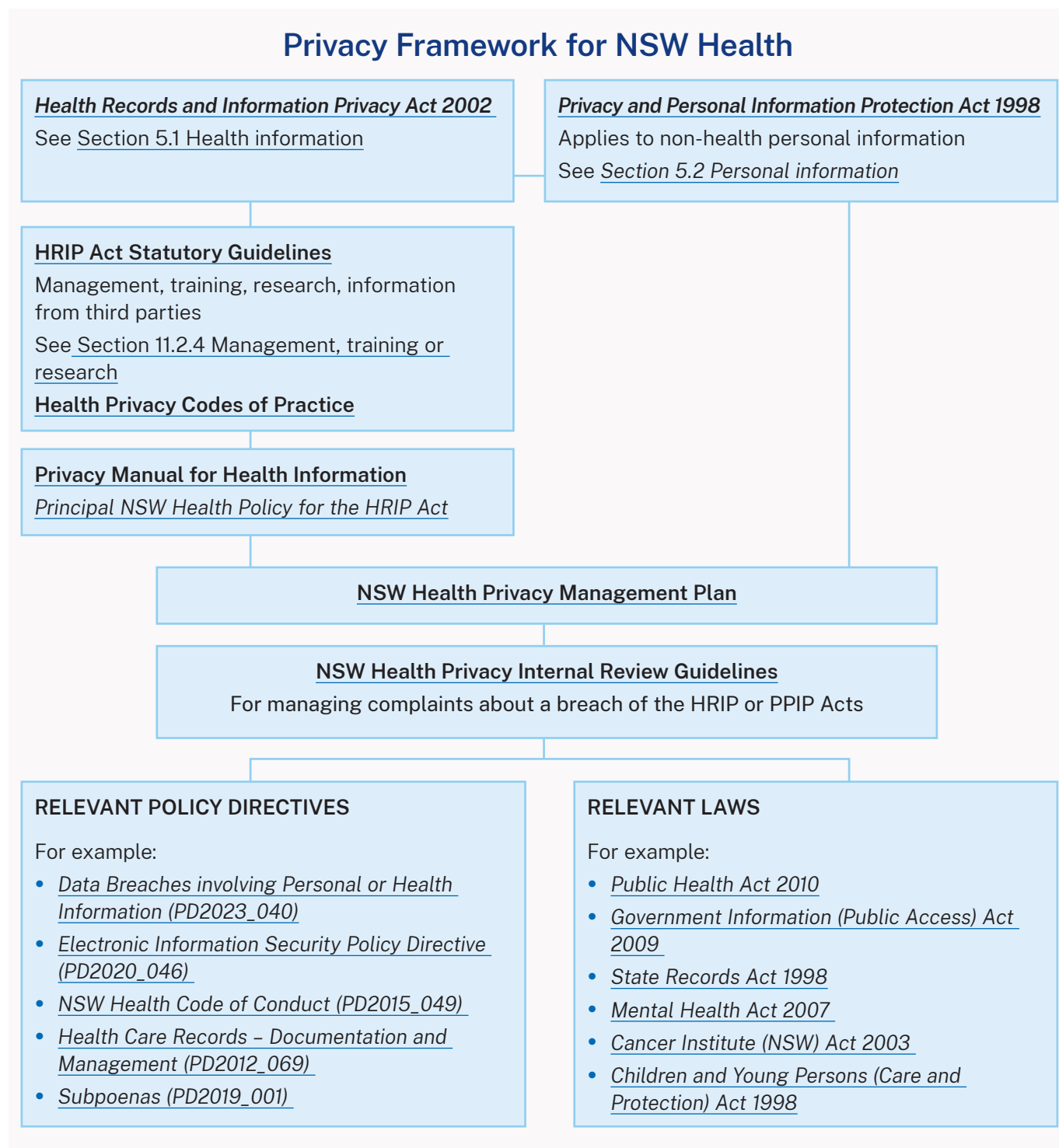


### 3.7 What other NSW Health resources should be considered

This Manual provides a broad overview of the key privacy obligations established under the [Health Records and Information Privacy Act 2002](#). There are however a range of other NSW Health policies which are also relevant to the collection, use, storage, and disclosure of information in NSW Health. The main policies are referenced in the body of the Manual.

### 3.8 Privacy Framework for NSW Health staff

To assist staff to identify which privacy legislation applies to their circumstances or to a particular issue at hand and where to go for further guidance, refer to the privacy framework (below) which is also published on the NSW Health website and NSW Health intranet privacy page.



# 4 Other obligations

## 4.1 Privacy laws and related legislation

Privacy obligations in NSW generally arise from two separate laws:

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

The Health Privacy Principles (HPPs) contained in the [Health Records and Information Privacy Act 2002](#) enable health services to lawfully collect, store, access, amend, use and disclose personal health information in prescribed circumstances. See Section 2.2 Summary of the HPPs.

There are, however, other pieces of legislation which impose specific controls on when and how information can be used and disclosed or allow for use and disclosure of information in certain circumstances. NSW Health also has a range of policies that impact on the use and disclosure of certain information.

A summary is set out below.

### 4.1.1 General secrecy provisions

NSW Health staff should be aware that almost all information (both personal and non-personal information) they have access to is subject to legislative provisions called 'secrecy' or 'non-disclosure' provisions. For example, see section 22 of the [Health Administration Act 1982](#), section 189 of the [Mental Health Act 2007](#) and section 130 of the [Public Health Act 2010](#). These provisions make it an offence to disclose information unless specified criteria are met. In general, these criteria include disclosures made in connection with the administration of the health related legislation, or with the consent of the person from whom the information was obtained or with other lawful excuse (e.g., pursuant to a court order) or in circumstances prescribed by regulations.

### 4.1.2 Mental health

The [Mental Health Act 2007](#) governs the way in which the care and treatment of people in NSW is provided to those people who experience a mental illness or mental disorder.

Division 2 of Chapter 4 of the [Mental Health Act 2007](#) deals with information sharing in the context of care and treatment. This division deals with sharing information with the patient, their carer or representative at a Mental Health inquiry or before the Mental Health Review Tribunal relating to medication, mental health inquiries, detention, movements, reclassification, and discharge of patients. There are also specific provisions giving primary carers the right to certain information, particularly in relation to notification of detention, ongoing care, and discharge planning.

Where patients are detained in a mental health facility, their legal representatives require access to the patient's records in order to properly represent the patient.

NSW Health has also entered into a memorandum of understanding (MOU) with the NSW Police Force in relation to mental health emergencies. This MOU provides for the collaborative management of persons who have a mental illness or mental disorder, or who exhibit behaviours of community concern and provides practical guidance on the circumstances when personal health information can be shared with the NSW Police Force, and examples of the types of relevant information that may be shared.



#### Further guidance:

- [NSW Health – NSW Police Force Memorandum of Understanding 2018](#)
- [Right to access medical records by legal representatives – Mental Health Review Tribunal hearings \(IB2018\\_019\)](#)
- [Mental Health Act 2007 Guidebook, February 2023](#)
- [Amendments to the NSW Mental Health Act \(2007\) – Carers and families](#)
- Section 11.2.8.2 What sort of information can be provided? (to law enforcement)

### 4.1.3 Serious adverse event reviews

The *Health Administration Regulation 2020* allows disclosure of information in certain circumstances where it is necessary to investigate a reportable incident or for the conduct of a serious adverse event review (such as a Root Cause Analysis).



#### Further guidance:

- [\*NSW Health Incident Management Policy directive \(PD2020\\_047\)\*](#)

### 4.1.4 Epidemiological information

The *Health Administration Regulation 2020* and the *Public Health Act 2010* allow the Health Secretary or the Chief Health Officer to authorise the release of epidemiological information subject to various conditions.



#### Further guidance:

- [\*PD2015\\_037: Data Collections – Disclosure of Unit Record Data held for Research or Management of Health Services\*](#)
- Section 15.14 – NSW data collections

### 4.1.5 HIV/AIDS-related information

An important confidentiality provision in the *Public Health Act 2010* deals specifically with 'HIV/AIDS-related information'. See Section 11.2.3.4 for information on the *Public Health Act 2010* limitations imposed on the disclosure of information indicating a person's HIV status, and information that a person has undergone an HIV test.



#### Further guidance:

- [\*NSW Health Guide to Managing HIV Information \(IB2019\\_004\)\*](#)
- Section 15.9.6 – Managing public health risks
- 11.2.3.4 Public Health Act 2010 limitations on disclosure of information indicating a person's HIV status

### 4.1.6 *Children and Young Persons (Care and Protection) Act 1998 (NSW)*

Health staff have mandatory reporting obligations to report children at risk of significant harm under the *Children and Young Persons (Care and Protection) Act 1998*.

Chapter 16A of the *Children and Young Persons (Care and Protection) Act 1998*, facilitates the exchange of information between prescribed agencies for the safety, welfare and wellbeing of a child or young person. Exchange of information in accordance with Chapter 16A does not constitute a breach of privacy laws. For further information about privacy and child protection, see section 11.3.2 Child protection.



#### Further guidance:

- Section 11.3.2 Child protection

### 4.1.7 *Crimes (Domestic and Personal Violence) Act 2007*

Part 13A of the *Crimes (Domestic and Personal Violence) Act 2007* deals with exchange of information between prescribed agencies. See section 11.3.5 for further information.

### 4.1.8 Privacy Act 1988 (Cth)

The Commonwealth privacy legislation is limited to the regulation of the Commonwealth public sector and the private sector, including GPs and non-government organisations. Its provisions relating to health information do not generally apply to NSW Health organisations.

NSW Health agencies should be aware that Commonwealth privacy legislation may bind non-government organisations and private sector health providers (such as individual health practitioners, private hospitals, and researchers), and so may be relevant to the way these individuals and organisations interact with NSW Health. These organisations (unless an exemption applies) are required to comply with the Australian Privacy Principles defined by the Commonwealth legislation, which are similar but not identical to the HPPs.

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

Health services should always be mindful that disclosures to Commonwealth agencies, as with all other agencies, must meet the standard limits for disclosure under the [Health Records and Information Privacy Act 2002](#).

#### 4.1.9 Mandatory reporting under Commonwealth legislation

The [Privacy Act 1988](#) also imposes mandatory requirements to report serious breaches of privacy to the Office of the Australian Information Commissioner (OAIC) and affected parties.

This does not apply to most information under the control of NSW Health as NSW Health organisations are largely exempt from the requirements of the [Privacy Act 1988](#).

NSW Health is only subject to mandatory data breach notification requirements under the [Privacy Act 1988](#) for breaches relating to Tax File Numbers (TFNs).

Local Health Districts and Specialty Networks should also be aware of reporting obligations that apply in relation to cyber incidents under the [Security of Critical Infrastructure Act 2018](#).



##### Further guidance:

- [IPC Fact sheet – NSW public sector agencies and data breaches involving tax file numbers](#)
- Section 11 Using & disclosing personal health information (HPPs 10 & 11)
- Section 13.2 Transferring personal health information outside of NSW (HPP 14)
- Section 14.4 Responding to data breaches

#### 4.1.10 My Health Records Act 2012 (Cth)

My Health Record is Australia's national electronic medical record system. All Australians have a My Health Record, unless they choose not to have one. For information about privacy aspects of My Health Record and HealtheNet, please see 16.8.1 Mandatory security and access requirements.



##### Further guidance:

- Section 14.4 Responding to data breaches
- Section 16.8 My Health Record
- [My Health Record Security and Access Procedure \(PD2019\\_054\)](#)
- [HealtheNet and My Health Record Clinical Guide](#)

#### 4.1.11 National Disability Insurance Scheme Act 2013 (Cth)

The [National Disability Insurance Scheme Act 2013](#) (NDIS Act) includes privacy provisions that apply to information about a person that is or was held in the records of the National Disability Insurance Agency (Agency) and information to the effect that there is no information about a person held in the records of the Agency. This information is referred to as 'protected Agency information' in the NDIS Act.

The privacy provisions in the NDIS Act also apply to 'protected Commission information' which includes information about a person (including a deceased person) that is or was held in the records of the NDIS Quality and Safety Commission.

For example, NDIS Plans fall within the definition of 'protected Agency information.' Consideration must be given to the strict privacy requirements under Chapter 4 Part 2 of the NDIS Act before NDIS Plans or information that is 'protected Agency information' or 'protected Commission information' is used or disclosed for purposes other than those under the NDIS Act.

If NDIS providers approach a health organisation for NDIS information or other patient health information, the health organisation should have the patient's written consent to release this information.

The Agency has a range of guidelines and supporting information about privacy and consent (including consent forms).

The NDIS operational guideline '[Your privacy and information](#)' describes how participant information is collected, used, kept secure and disclosed according to the [Privacy Act 1988](#) and the NDIS Act. The consent forms that the guideline refers to are available on the NDIS website. If information is required from the Agency, staff are advised to obtain written consent from the participant for the Agency to exchange information with all staff employed by a local health district rather than just an individual staff member.

There is also a NDIS information sharing protocol that guides the release by the Agency to state and territory agencies. See: [Sharing information about participants, prospective participants and providers with third parties](#). This protocol acknowledges a limited set of circumstances where information may need to be released by the Agency without the participant's explicit consent, such as a person being admitted to hospital who is unable to provide consent and does not have a known authorised representative. This is essentially an 'emergency scenario' and may be supported under NSW privacy legislation and the NDIS Act. The protocol gives guidance and tools to seek release of information in these circumstances.



In addition, if a subpoena requests NDIS-specific documents (e.g. a patient's NDIS Plan) it is appropriate to refer the requestor to the Agency as the owner of the document.



#### Further guidance:

- [NDIA, Sharing information about participants, prospective participants and providers with third parties](#)
- [NDIS Consent forms](#)

## 4.2 Other laws regulating information management

### 4.2.1 [State Records Act 1998 \(NSW\)](#)

The [State Records Act 1998](#) provides for the creation, management, and protection of the records of public offices of the State and for public access to those records.

The [State Records Act 1998](#) overlaps with the [Health Records and Information Privacy Act 2002](#) in relation to the retention and disposal of records held by public sector agencies and public access to those records.

Public sector agencies must comply with the requirements of both Acts.



#### Further guidance:

- [Section 9.1 Retention and disposal of personal health information](#)

### 4.2.2 [Government Information \(Public Access\) Act 2009 \(NSW\) \(GIPA Act\)](#)

The GIPA Act allows any person to apply for access to any information held by government. It is different from the [Health Records and Information Privacy Act 2002](#) as it is designed to facilitate open and transparent government and is not restricted to personal information, whereas privacy laws are designed to provide individuals with greater knowledge and control over their own information. Under a GIPA Act application or privacy request, staff details including name and work contact details, may be released to the applicant or complainant. Where there are concerns for safety, they should be addressed on a case-by-case basis. For further information about privacy and the GIPA Act, see section 12.2 *Interaction of privacy law and the GIPA Act*.



#### Further guidance:

- [Section 12 Patient access and amendment \(HPPs 6, 7 & 8\)](#)
- [Government Information \(Public Access\) Act 2009](#)

## 4.3 Common law, professional and other obligations to protect privacy

The [Health Records and Information Privacy Act 2002](#) requires staff to protect the privacy of health information and the [Privacy and Personal Information Protection Act 1998](#) requires staff to protect all other personal information, such as staff records.

Section 68 of the [Health Records and Information Privacy Act 2002](#) provides offences for public sector officials who intentionally disclose or use health information without authorisation. Penalties include a fine of up to \$11,000 or imprisonment for up to 2 years, or both. The [Privacy and Personal Information Protection Act 1998](#) also contains a similar offence.

### 4.3.1 Duties of confidentiality

Health care providers also owe patients a common law duty of confidentiality in relation to information obtained as part of the treating relationship. The duty is based in part on contract law and on the 'fiduciary duty' of an individual practitioner to his or her patients. The duty is not absolute and there are circumstances where a provider may disclose the information without breaching common law duties. These exceptions are similar to the main exceptions in the [Health Records and Information Privacy Act 2002](#) relating to consent, threats to health and safety, law enforcement and requirements of other legislation.

Although these common law obligations continue to apply to individual health professionals, the provisions of the [Health Records and Information Privacy Act 2002](#) have in effect replaced the common law regarding personal health information for most NSW Health purposes.

### 4.3.2 [NSW Health Code of Conduct](#)

The [NSW Health Code of Conduct \(PD2015\\_049\)](#) defines standards of ethical and professional conduct that are required of everyone working in NSW Health. Chief Executives are responsible for ensuring that the Code is promoted throughout their agency.

The [NSW Health Code of Conduct \(PD2015\\_049\)](#) requires a standard of behaviour which demonstrates respect for the rights of the individual and the community and maintains public confidence and trust in the work of the public health system. Section 4.5 of the Code of Conduct includes requirements for observing the privacy, confidentiality and security of information obtained during employment within NSW Health. Staff must maintain the security of confidential and/or sensitive official information. Staff must:

- Keep confidential all personal information and records, including not discussing or providing information on social media that could identify patients or divulge patient information
- Not use or release official information or records without proper authority
- Maintain the security of confidential and / or sensitive information, including that stored on communication devices
- Not disclose, use, or take advantage of information obtained in the course of official duties, including when they cease to work in NSW Health.

#### 4.3.3 Registered health professionals

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

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

#### 4.3.4 Disciplinary matters and ICAC reporting

Privacy breaches committed by staff may require a disciplinary response and consideration of notification to the [Independent Commission Against Corruption \(ICAC\)](#). Legal advice should be sought from the Ministry of Health in relation to serious breaches that may require referral for prosecution.

It is important that there is coordination of the privacy response, the staff misconduct response and consideration of the ICAC response across the organisation. These functions are generally performed by the Privacy Contact Officer, human resources and Internal Audit teams respectively. Actions taken should be commensurate with the nature, scale, and seriousness of the breach.

Referral of staff to human resources for investigation, under NSW Health Policy directive [Managing Misconduct \(PD2018\\_031\)](#), must be considered in any instance of unauthorised staff access to personal or health information where a staff member knows that this conduct is unauthorised.

All staff working for NSW Health are bound by the [Independent Commission Against Corruption \(ICAC\) Act 1988 \(NSW\)](#). Corrupt conduct includes where a staff member knowingly and intentionally accesses, uses or discloses information held by a health service for a purpose outside of work duties. This may also constitute an offence under the [Crimes Act 1900](#), the [Health Records and Information Privacy Act 2002](#) and/or the [Privacy and Personal Information Protection Act 1998](#). Principal Officers of NSW Health agencies are required to report all instances of corruption to ICAC where there is a reasonable suspicion that corrupt conduct has, or may have, occurred.



#### Further guidance:

- NSW Health Policy directive, [Managing Misconduct \(PD2018\\_031\)](#)
- [NSW Health Code of Conduct \(PD2015\\_049\)](#)
- NSW Health Policy directive, [Corrupt Conduct – Reporting to the Independent Commission Against Corruption \(ICAC\) \(PD2016\\_029\)](#)
- Section 14 Complaints handling and responding to breaches

# 5 Key concepts

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

## 5.1 Health information

Health information is personal information or an opinion about:

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

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

The [Health Records and Information Privacy Act 2002](#) also specifically includes personal information that is genetic information about an individual that predicts or could predict the health of the individual or of their genetic relatives. A genetic relative means a person who is related to an individual by blood, for example, a sibling, parent, or descendant of the individual. See Section 11.2.3.5 Genetic information.

An Individual Health Identifier (IHI) issued by the Commonwealth under the [Healthcare Identifiers Act 2010](#) is also health information.

Under the [Health Records and Information Privacy Regulation 2022](#), a health service includes:

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

The [Health Records and Information Privacy Act 2002](#) uses the term 'health information' to mean health information that is also personal information - meaning it identifies or could potentially identify an individual. This Manual has, however, adopted the term 'personal health information,' to emphasise that neither the [Health Records and Information Privacy Act 2002](#) nor the Manual regulates the collection, use or disclosure of other health-related but non-identifying information, such as de-identified and statistical data. The requirements of the Manual do not need to be followed in relation to this type of information. However, to de-identify personal health information the HPPs must be complied with.



### Further guidance:

- [NSW Health Policy Directive, Data Collections – Disclosure of Unit Record Data for Research or Management of Health Services \(PD2015\\_037\)](#)
- See section 5.3, De-identified information
- Section 11.2.5 Management, training, or research HPPs 10 & 11 (1) (d), (e) & (f)

## 5.2 Personal information

Personal information is defined in Section 4 of the [Privacy and Personal Information Protection Act 1998](#) as: 'Information or an opinion (including information or an opinion forming part of a database and whether or not recorded in material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.'

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

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



### Example

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

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

The definition of personal information is much broader than that of personal health information and is regulated by the [Privacy and Personal Information Protection Act 1998](#). The legislative requirements for managing general personal information are different from the requirements for managing personal health information and are not covered by this Manual. Guidance for NSW Health staff on the management of personal information is contained in the [NSW Health Privacy Management Plan](#).



#### Further guidance:

- [NSW Health Privacy Management Plan](#)

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

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

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

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

## 5.3 De-identified information

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

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

### Example

Data on small or unique groups, particularly in rural areas, may not be de-identified even where identifiers have been stripped. A person's identity may be apparent where neither their name nor an image or photograph is available, but the information about the person is such that it could be unique enough to identify them. For this reason, care needs to be taken when managing the de-identification of any personal or health information, particularly in small or unique groups.

Data on a rare cancer when analysed from a state-wide perspective may not be identifiable but when viewed at District level or in a smaller data cohort, then patient identity may be identifiable, in which case the Health Privacy Principles should be applied.

The [Commonwealth's Office of the Australian Information Commissioner \(OAIC\)](#) suggests the following approach in satisfying a requirement for de-identification: De-identification involves two steps. The first is the removal of direct identifiers. The second is taking one, or both, of the following additional steps:

- the removal or alteration of other information that could potentially be used to re-identify an individual (DOB, MRN or other unique identifiers, for example) and/or
- the use of controls and safeguards in the data access environment to prevent re-identification

De-identified information is exempt from privacy laws and from the requirements of this Manual, but care should be taken to consider any potential risks of re-identification, particularly in circumstances where the data context changes. The Health Privacy Principles do not apply to de-identified information. However, using or disclosing health information for the purpose of de-identification (e.g. for research, training and management of health services) must

be in accordance with the HPPs and any relevant Statutory Guidelines issued by the Privacy Commissioner.



#### Further guidance:

- [A framework for data de-identification](#), OAIC and the CSIRO
- [Fact sheet: de-identification of personal information](#), Information and Privacy Commission (IPC)
- [Privacy issues and the reporting of small numbers](#), HealthStats NSW, NSW Health

## 5.4 Consent

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

### 5.4.1 Elements of consent

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

of time has passed, or the patient's personal situation has changed so markedly that there are grounds to suggest their views may have changed.

- Consent can be obtained **in writing or verbally in person or by audio-visual link**, but when obtained verbally should always be recorded, for example, by a notation in the patient's health record. Reasonable steps must be taken to ensure that the reason that we are obtaining consent is clearly articulated in the terms of the consent..

### 5.4.2 Implied consent

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

#### Example

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



#### Further guidance:

- [NSW Health Consent to Medical and Healthcare Treatment Manual \(Consent Manual\)](#)

### 5.4.3 Express consent

Express consent generally requires documentation showing specific and clear intention on the part of the patient. Express consent means consent that is clearly and unmistakably communicated so that it is clear to the patient (or their representative) what they are consenting to. The organisation must have gone to the individual concerned (or their representative) and obtained an express consent that is precise as to the kind and contents of the information to which the consent relates.

This requirement could be met by a formal written consent, including a handwritten signature, an oral statement, or use of an electronic medium or voice signature to signify agreement, provided the description of the activity being consented to is accurate, precise, and clearly expressed. The [Health Records and Information Privacy Act 2002](#) requires 'express consent' from the patient in the following circumstances:

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

In circumstances where an oral statement is made, it must be recorded or documented in a record.

#### 5.4.4 Deciding if consent is needed

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

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

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

- access to the information is being requested under a court subpoena or search warrant;
- release of a discharge summary to a patient's GP (General Practitioner) where the patient (or their authorised representative) has provided the GP's details;

- for current and future ongoing care and treatment purposes where the patient has been made generally aware that their information may be used in this way;
- use and disclosure of a patient's genetic information is permitted to their genetic relatives in certain circumstances prescribed in guidelines issued by the NSW Privacy Commissioner, Information and Privacy Commission NSW (see Section 11.2.3.5 Genetic information and below).

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



#### Further guidance:

- [Information and Privacy Commission, Fact sheet, Consent, and bundled consent, 2019](#)
- [Use and disclosure of genetic information to a patient's genetic relatives: Guidelines for organisations in NSW](#)

## 5.5 Test for capacity

### 5.5.1 General rule

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

The [Health Records and Information Privacy Act 2002](#) establishes considerations for assessing capacity, which provide that a person is incapable of giving consent (despite the provision of reasonable assistance by another person) if due to age, injury, or illness, or physical or mental impairment (temporary or otherwise), they:

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

These considerations do not therefore impose arbitrary rules (such as reaching a certain age) dictating capacity. Rather, it requires a professional assessment (generally from within the health organisation) of the individual's ability to make a specific decision at a point in time. The complexity, seriousness and long-term impact of any decision will impact on the level of understanding required in any particular case.

### 5.5.2 Minors

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

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

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

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

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

If an application for access to a minor's health information is received from a parent or guardian, in addition to considering the minor's capacity it is also important to consider whether there are any factors, such as risk of harm, which may mean access to health information should be refused. See 12.3.1 Reasons for refusing access.



#### Further guidance:

- Section 5.6.1.2 Where the health service is aware that parents are divorced or separated
- Section 7.4.7 Youth-friendly privacy resources

While specifically related to consent to treatment, there is further guidance on Minors and Consent in the NSW Health [Consent to Medical and Healthcare Treatment Manual](#)

## 5.6 Authorised representative

The concept of 'authorised representative' is an integral component of health privacy law.

An authorised representative can make decisions relating to access to, or disclosure of, health records on the patient's behalf where the patient lacks capacity to make these decisions for themselves (see Section 5.5 Test for capacity).

In order to ascertain who may act as a patient's authorised representative, health services should not rely on the person indicated in the health record as 'person to contact' or 'next of kin.' It is generally necessary to review a patient's health record to determine who may be appointed as their authorised representative, in accordance with the hierarchy set out in the [Health Records and Information Privacy Act 2002](#) below (see Section 5.6.1 Definition of an authorised representative').

Appropriate personal identification and any relevant documentation (for example, current enduring power of attorney, enduring guardianship documents) should be provided prior to the disclosure of, or access to, personal health information relating to a patient.

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

### 5.6.1 Definition of an 'authorised representative'

The [Health Records and Information Privacy Act 2002](#) sets out the list of people who can be an authorised representative on behalf of a patient who lacks capacity. They are:

- someone who has an 'enduring power of attorney' for the individual; or
- a guardian, including someone with 'enduring guardianship,' as defined in the [Guardianship Act 1987](#); or
- if the individual is a child under 18, a person who has parental responsibility for them. The Act



defines this as ‘all the duties, powers, responsibility and authority which, by law, parents have in relation to their children;’ or

- a ‘person responsible’ under Section 33A of the Guardianship Act 1987 (see 5.6.1.1); or
- any other person who is authorised by law to act for or represent the person.

Generally, the role of an authorised representative lapses when the patient dies. Powers of attorney, for example, have no effect after the person who made them has died.



#### Further guidance:

- Section 15.10 Deceased patients

##### 5.6.1.1 Defining a ‘person responsible’

A ‘person responsible’ for an individual other than a minor is determined by a hierarchy set out by the Guardianship Act 1987, as follows:

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

Despite the above hierarchy, the person responsible for a minor will be:

- the person with parental responsibility under the Children and young Persons (Care and Protection) Act 1998 for the minor,
- the Minister if the child is in the care of the Minister, or

- the Secretary if the child is in the care of the Secretary.
- Further, if the person is in the care of the Secretary under s 13 of the Guardianship Act 1987, the Secretary is the person responsible.

In circumstances where a family member who is not the authorised representative is seeking access to the health records of a patient who is at the end of their life and/or has lost capacity or is deceased, consideration may be given to disclosure of health information on compassionate grounds (see 11.2.10.)



#### Further guidance:

- Section 1 Definitions and acronyms
- Section 11.2.2.1 Where a third party seeks access
- Section 11.2.10 Disclosure on compassionate grounds
- Section 12 Patient access and amendment (HPPs 6, 7 & 8)

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

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

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



#### Further guidance:

- Section 5.5.2 Minors
- Section 12.3.1.3 The disclosure of personal information about a child would not be in the best interests of the child
- Section 12.5.1 Parenting orders

##### 5.6.1.3 Next of kin

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

The *Health Records and Information Privacy Act 2002* does not use or rely on the term 'next of kin.' It does not therefore give a 'next of kin' any authority to make decisions on behalf of the patient. Where a person is listed as a 'next of kin', the health practitioner should check whether they are an authorised representative (see above) before relying on that person to make a decision on behalf of the patient.

The term 'next of kin' has legal effect only in relation to deceased persons for some specific purposes. The term may apply to organ donation, coronial matters, autopsy consent, funeral arrangements and property matters following a person's death, but it does not apply to decisions that need to be made while the person is alive.



#### Further guidance:

- [\*Identifying the Carer at Patient Registration \(IB2019\\_031\)\*](#)
- [\*Coroners Cases and the Coroners Act 2009 \(PD2010\\_054\)\*](#)

## 5.7 'Reasonable' and 'practicable'

The *Health Records and Information Privacy Act 2002* often qualifies requirements by reference to what is reasonable or practicable. These are concepts that cannot be readily defined as they will vary depending on the particular circumstances arising. There are however certain matters which can be considered in deciding if something is 'reasonable' or 'practicable'.

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

## 5.8 'Sensitive' information and patient expectations

All personal health information is considered to be sensitive personal information, dealing with matters that are personal and which a patient will generally expect to be shielded from public disclosure. The terms of the *Health Records and Information Privacy Act 2002* are based on adopting and reflecting these expectations. The *Health Records and Information Privacy Act 2002* does not classify certain types of personal health information as being more sensitive than other types. However, there may be other statutory obligations that require certain types of information receive a greater level of protection, for example,

- HIV/AIDS-related information, see Section 4.1.5
- Adoption information, see Section 15.9.2
- Sexual assault communications privilege, see Section 15.13.3

The *Health Records and Information Privacy Act 2002* requires that personal health information be treated in accordance with an individual's reasonable expectations, and that reasonable steps are taken to inform a patient of how he or she can expect their information to be handled.

Health staff should be aware that some patients will not share the same general expectations as other patients for a variety of reasons, for example, if they have previously received health care in a different country, or if they are particularly sensitive about aspects of their health care. Health staff should not make assumptions about what a patient might consider 'sensitive.'

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

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



#### Further guidance:

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

### 5.8.1 Specific health services

In the case of some specific health services, such as genetics services or sexual health services, it may be appropriate to manage personal health information differently, given the more sensitive nature of the

information and the patients' expectation as to how their personal health information may be handled in these circumstances.



#### Further guidance

- Section 15.9 Information-specific laws and policies

### 5.8.2 Patient requests

In rare circumstances, a patient may make a special request that their personal health information is not used or disclosed for purposes as allowed by the [Health Records and Information Privacy Act 2002](#) and described in this Manual. When health service staff receive such a request, it will be situation specific and the professional judgment of local health service staff will be required to resolve such requests, for example, it may be necessary to balance the implications of meeting the request with the capacity to provide safe and appropriate health services.



#### Further guidance:

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

### 5.8.3 Non-personal 'sensitive' information

NSW Health agencies may hold sensitive information which is not personal health information, such as tender documents, private hospital licensing information or documents detailing government relations. These documents require secure document management in accordance with the [State Records Act 1998](#) including the relevant General Retention and Disposal Authority ([GDA 21 Public health administration records](#)). This authority applies to records created and maintained to support the management and delivery of public health care services and programs. Where, as in most cases, these documents do not contain personal health information, the terms of the [Health Records and Information Privacy Act 2002](#) and this Manual will not apply.

The GIPA Act may also be relevant in circumstances where members of the public seek access to this type of non-personal 'sensitive' information.



#### Further guidance:

- Section 4.2.2 [Government Information \(Public Access\) Act 2009](#)
- For GIPA enquiries [contact the Ministry of Health GIPA team](#).



# 6 Responsibilities under privacy law

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

It is essential that health staff be made aware of their individual rights and responsibilities in respect of safeguarding the privacy of patient information. Staff must only access patient information in the course of their employment and for patient care purposes.

Staff need to be informed about patients' rights of privacy and the processes in place to manage access to information requests, queries, and complaints (including their own rights of privacy).

The importance of common-sense privacy precautions cannot be over-emphasised, such as not discussing patients publicly in a manner that would allow identification of individuals or small groups, taking care to ensure the security of information when working out of office or at home, keeping passwords secure, not sharing log-in details, and taking measures to ensure patient information in electronic health record systems is secure and protected from unauthorised access. Staff should log out of their computers at the end of every shift and secure any workstations when they are not in use.

Staff should also be aware that they are not authorised under privacy law to informally access a family member's or friend's health information, or even their own personal health information. Such access is a breach of the [NSW Health Code of Conduct](#). All staff need to make a formal application to their Health organisation's Health Information Service to seek access to these types of records. If in doubt, check with a senior manager. This is to prevent staff from accessing information that is not related to their work and protects staff from potential complaints that may be made.

## 6.1 Chief Executives

### 6.1.1 Key obligations

- to ensure all staff members are aware of the requirements of this Manual;
- to ensure all staff members undertake appropriate privacy training;
- to ensure all staff members have access to appropriate material about their privacy obligations, including the [NSW Health Privacy Leaflet for Staff](#), the Privacy Manual for Health Information, and the [NSW Health Privacy Management Plan](#);

- to meet annual reporting requirements regarding privacy compliance and applications for internal review (see Section 6.7 Privacy annual reporting);
- to manage and appropriately escalate any data and cyber security breaches and to comply with the NSW [Mandatory Notification of Data Breach Scheme](#) and other mandatory reporting obligations;
- to understand any mandatory breach reporting requirements relating to Tax File Numbers (see Section 14.4) and the [My Health Records Act 2012](#) (See Section 4.1.8);
- to designate a specific officer (or Privacy Contact Officer) for the health service to whom requests for guidance on information privacy should be referred and who should support staff in ensuring privacy policies and procedures are observed.



#### Further guidance:

- [NSW Health Privacy Management Plan: Information Bulletin \(IB2023\\_012\)](#)
- [Data Breaches involving Personal or Health Information \(PD2023\\_040\)](#)
- NSW IPC [Mandatory Notification of Data Breach Scheme](#)

### 6.1.2 Staff training

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

All staff should be provided with the NSW Health [Privacy Leaflet for Staff](#).

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

Two privacy online training modules are also available via the [My Health Learning portal](#) or the NSW Health Education and Training Institute (HETI).

### 6.1.3 Mandatory training

All NSW Health staff are required to complete one privacy online training module and the 'Cyber Security Fundamentals' e-module as part of their mandatory training requirements.

A newer module 'Cyber Security Awareness for NSW Health' is highly recommended and complements the Cyber Security Fundamentals module. It is a 35-minute e-module targeted to all staff. The module is accessible via My Health Learning and compulsory completion is determined by the local Chief Executive of each health organisation.

The mandatory privacy training module is entitled 'Privacy module 1 – Privacy – It's yours to keep'. This training module takes approximately 20 minutes to complete. Staff should undertake this training as part of orientation within one month of commencement as a NSW public health system employee.

The second 'My Health Learning' privacy Module, 'Privacy Module 2 – Handling Personal & Health Information', while not mandatory, is relevant to any staff member who handles personal or health information.

There are further courses available via My Health Learning that have relevance to Privacy. The course [Use and Disclosure of NSW Health Data for the Purpose of Analytics](#) identifies the practices that help maintain the privacy, integrity and security of data held in NSW Health data collections. This would be useful to any staff member using or accessing NSW Health data collections. There is also a course on 'Privacy and Dignity' which focuses on ways to deliver greater privacy and dignity to patients. Also available on My Health Learning is an additional privacy module – Cyber S.A.F.E – Information Privacy – Protecting Data.



#### Further guidance:

- [Mandatory Training – Criteria for Approval as an NSW Health Requirement \(PD2016\\_048\)](#)

### 6.1.4 Staff communication and alerts

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

Building alerts, undertakings and notifications into electronic systems may also assist to inform staff of their privacy obligations. Providing staff with brief

privacy messages at critical decision points in the system may be an effective way of reminding staff of privacy obligations and ensuring privacy is always considered.

Some examples of electronic notifications for NSW Health staff are:

- Remember you must only access the information necessary to fulfil your work duties. If in doubt, check with your senior manager. For further guidance, see: [NSW Health Patient privacy](#)
- You are bound by strict privacy laws and NSW Health privacy policies regarding access to, use and disclosure of the personal health information contained within the NSW Health system.
- The principal NSW Health privacy policy is the [NSW Health Privacy Manual for Health Information](#).
- The principal privacy law for patient information is the [Health Records and Information Privacy Act 2002](#)
- If you suspect a breach of the privacy or security of the NSW Health system, you should discuss this with your manager, and consider contacting the [Privacy Contact Officer for your organisation](#).

See pro forma privacy undertakings on the NSW Health intranet privacy webpage and NSW Health Policy Directive, [Use & Management of Misuse of NSW Health Communications Systems \(PD2009\\_076\)](#).

## 6.2 Privacy Contact Officer

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

Privacy Contact Officers would usually be involved with:

- **Supporting staff**
  - Acting as a first point of contact for staff and members of the public for matters related to privacy.
  - Supporting staff in implementing and following privacy policies and guidelines, leading privacy education, and promoting a privacy-aware culture across the organisation.
- **Liaison with NSW Information and Privacy Commission**
  - Acting as a first point of contact with the NSW Information and Privacy Commission, recognising that the chief executive is the delegate signatory for all correspondence with the Commission, the Secretary and Deputy Secretaries.

- **Internal Reviews, Appeals and Complaints**

- Ensuring privacy complaints and requests for privacy internal review are dealt with in accordance with the [NSW Health Privacy Internal Review Guidelines \(GL2019\\_015\)](#) and statutory requirements, recognising the role of the Audit and Risk Management Committee (ARMC) and Chief Audit Executive in oversight of statutory compliance.
- Notifying the Ministry of Health Privacy Contact Officer of all HRIP Act internal reviews.
- Notifying the Ministry of Health legal team of all privacy internal reviews involving significant legal matters.
- Notifying the Ministry of Health legal team of all NCAT appeals of privacy internal reviews so that appropriate legal representation can be arranged.



**Further guidance:**

- See section 14.3, NSW Civil and Administrative Tribunal
- See sections 5.6 and 7.11, [Privacy Internal Review Guidelines \(GL2019\\_15\)](#)
- [Significant Legal Matters and Management of Legal Services \(PD2017\\_003\)](#)
- **Data breaches**
  - Ensuring compliance with [Data Breaches involving Personal or Health Information \(PD2023\\_040\)](#)
  - Notifying all suspected data breaches involving NSW Health information systems to the Security Investigations Team of eHealth NSW through either SARA or the State-Wide Service Desk **1300 28 55 33**, or by email: [EHNSW-IS-SECURITY-Incidents@health.nsw.gov.au](mailto:EHNSW-IS-SECURITY-Incidents@health.nsw.gov.au).
  - Advising staff on obligations to manage and report certain privacy or data breaches as corporate incidents under the [NSW Health Incident Management Policy directive \(PD2020\\_047\)](#)
- **Disciplinary matters**
  - Referring incidents of unauthorised staff access to personal or health information to the organisation's human resources unit for consideration of disciplinary action (as required by Managing Misconduct Policy directive (PD2018\_031) in circumstances where a staff member accesses information knowing that the access is unauthorised.

- **Privacy Annual reporting requirements**

- Preparing the organisation's annual privacy submission to the Ministry of Health, and ensuring the information is published on the organisation's website in the specified timeframes.



**Further guidance:**

- Contact details for [NSW Health Privacy Contact Officers](#).

## 6.3 Other staff

### 6.3.1 Managers and supervisors

- should provide leadership and direction to ensure the Manual is effectively implemented in the units or by the staff they are responsible for
- should monitor the quality and effectiveness of management and use of personal health information and take appropriate action to address any risks, gaps or shortcomings
- should ensure staff responsible for management and use of personal health information have the skills and support they need to effectively comply with privacy law, including access to privacy education and training
- should include privacy provisions in policies, procedures and plans wherever appropriate
- should refer privacy complaints and requests for privacy internal review to the Privacy Contact Officer for the health service
- should be aware of local protocols as to when to refer requests for access to and disclosure of personal health information to the local Health Information Service.
- where there is an incident, be aware of other obligations arising under the:
  - [NSW Health Code of Conduct \(PD2015\\_049\)](#)
  - [NSW Health Policy Directive Electronic Information Security \(PD2020\\_046\)](#)
  - [NSW Health Incident Management Policy directive \(PD2020\\_047\)](#)

### 6.3.2 Health care providers

- should take responsibility for implementing and complying with the [Health Records and Information Privacy Act 2002](#) and this Manual and for keeping up to date with any changes
- should refer privacy complaints or concerns about handling of health information to the Privacy Contact Officer for the health service. See Section 14 Complaints handling and responding to breaches.

### 6.3.3 Funding and grants administrators

- should ensure funding processes, conditions and reporting requirements comply with privacy law
- should monitor the protection of personal health information in programs and initiatives funded by the public health system and initiate appropriate action to address any risks or shortcomings
- should ensure a Privacy Impact Assessment for new projects or initiatives is conducted, where appropriate.

### 6.3.4 Information systems and information technology (IT) managers

- should ensure that the development and modification of IT systems comply with privacy law
- should ensure that all documentation and processes for IT policy, procedures and governance are consistent with privacy law
- should ensure a Privacy Impact Assessment for new projects or initiatives is conducted, where appropriate



#### Further guidance:

- [IPC Guide to Privacy Impact Assessments in NSW](#)
- [NSW Health Policy Directive Electronic Information Security \(PD2020\\_046\)](#)

## 6.4 Contracted agencies

A responsible representative of a contracted agency, where the service necessitates accessing personal health information, should sign an undertaking to comply with the [Health Records and Information Privacy Act 2002](#) or equivalent law as part of the conditions of their contract. The agreement should clearly set out responsibility for data security in transit and requirements for secure storage. Individuals working for the contracted agency should also sign undertakings where their tasks will involve direct access to personal health information.

Any undertakings should be adapted to local needs with consideration of the personal and health information the individual may have access to for the purpose of their role. Further guidance should be sought from those supervising the staff (or contractors) and prepared in consultation with the Privacy Contact Officer for the health organisation or Data Custodian for a recognised data set/asset.

Examples of key privacy criteria appropriate for inclusion are as follows:

- an undertaking not to knowingly access any

personal health information unless such information is essential to perform contractual obligations properly and efficiently

- an understanding that access to, holding and use of personal health information is subject to the Health Privacy Principles contained in the [Health Records and Information Privacy Act 2002](#)
- an undertaking to comply with the Health Privacy Principles and relevant NSW Health policies affecting the collection, holding, use or disclosure of personal health information
- an undertaking not to divulge any personal health information regarding individual persons, except as allowed by the Health Privacy Principles
- an undertaking to follow other information privacy and security procedures as stipulated by NSW Health policies in relation to any personal health information accessed during contractual obligations
- an undertaking to ensure that, as far as is possible, such information, whether in the form of paper documents, computerised data or in any other form, cannot be viewed by unauthorised persons, and that the information is stored in a secure and orderly manner which prevents unauthorised access
- an undertaking to inform a supervisor/NSW Health contact immediately in the event of any breach of privacy or security relating to personal health information accessed in the course of contractual obligations.

The above criteria are set out in the [NSW Health Privacy Undertaking template](#) and can be amended or deleted as appropriate, depending on the role and the types of information the staff member/contractor will have access to. However, the general obligations in the undertaking should not be amended or deleted without advice from the Ministry of Health legal team. If the staff member/contractor has access to multiple systems or datasets containing personal and health information, consideration should be given to listing each system or dataset in the undertaking.

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



#### Further guidance:

- [NSW Health Privacy Undertaking template](#)
- [NSW Health Data Governance Framework \(GL2019\\_002\)](#)
- [Disclosure of unit record data by Local Health Districts for research or contractor services \(PD2018\\_001\)](#)



## 6.5 Compliance tips

There are a number of ways health services can support their staff to meet the obligations under the [\*Health Records and Information Privacy Act 2002\*](#).

Options include:

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

## 6.6 NSW Health privacy webpage and key privacy resources

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

Key privacy resources include:

- [\*NSW Health Policy Directive Electronic Information Security \(PD2020\\_046\)\*](#)
- [\*NSW Health Privacy Internal Review Guidelines \(GL2019\\_015\)\*](#)
- [\*NSW Health Privacy Management Information Bulletin \(IB2023\\_012\)\*](#)
- [\*NSW Health Code of Conduct \(PD2015\\_049\)\*](#)
- [\*NSW Government Cyber Security Policy\*](#)
- [\*NSW Health Data Governance Framework \(GL2019\\_002\)\*](#)
- [\*NSW Health Policy Directive, Use & Management of Misuse of NSW Health Communications Systems \(PD2009\\_076\)\*](#)
- [\*NSW Health Privacy Management Plan\*](#)
- [\*NSW Health Privacy Leaflet for Patients\*](#)
- [\*NSW Health Privacy Leaflet for Staff\*](#)
- [\*NSW Health Privacy webpage\*](#)

## 6.7 Privacy annual reporting

To support NSW Health to meet its annual reporting obligations, each NSW Health organisation is to provide a submission to the Ministry of Health (via email [MOH-Privacy@health.nsw.gov.au](mailto:MOH-Privacy@health.nsw.gov.au)) by 31 July each year, outlining the actions it has undertaken in relation to privacy management and compliance, and details of privacy statistics, for the financial year immediately prior. A template is distributed to provide guidance on the content of the submission.

From 2024, information reported to the Ministry is consolidated for inclusion in the NSW Health Annual Report.

All NSW Health organisations are to publish their own privacy management actions and statistics (as included in the submission to the Ministry) on their own internet websites after the NSW Health Annual Report has been published on the NSW Health internet website, and by no later than 30 November of that same year (unless otherwise advised by the Ministry).

# 7 Collecting personal health information (HPPs 1 – 4)

Everyone who has direct contact with patients may have some role in collecting personal health information. Those not involved in direct service provision, such as admissions clerks, may also collect health information from patients. Sometimes NSW Health workforce teams also collect personal health information from staff related to their employment.

## 7.1 When can you collect information? (HPP 1)

HPP 1 requires agencies to only collect health information for a lawful purpose that is directly related to the agency or organisation's activities and necessary for that purpose.

Privacy laws allow health services and health staff to collect personal health information for purposes relating to health care, treatment, and other ancillary/support services.

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

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

When collecting personal health information, you should consider these functions. Information should only be collected if the purpose of collection is directly related to what the agency does, and the collection is necessary for those purposes or another lawfully authorised purpose. Further, the use and disclosure of the information collected may fall

within the exemption for the management of health services but should be considered with reference to the Statutory Guidelines (see Section 11.2.5 Management, Training, or Research).

### Example

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

Information cannot be collected by an 'unlawful means'.

### Example

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

## 7.2 How should information be collected? (HPP 2)

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

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

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

### Example

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

### Example

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

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

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

### Example

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

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

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

### Examples

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

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

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

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

## 7.4 Informing individuals about what is collected (HPP 4)

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

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

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

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

Those examples of most relevance to health services are set out here:

#### 7.4.1.1 The person to whom the information relates lacks capacity

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

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

#### 7.4.1.2 The person waives their right to be told

If the person expressly waives their right to be told information regarding the collection, security, use and disclosure of their personal health information, HPP 4 does not need to be complied with.

HPP 4 requires this waiver to be by 'express consent'. Express consent must be verbal or in writing. Any such waiver should be recorded by making a note on the medical record to document a verbal consent or recording of written consent to enable later verification. Staff may also need to consider the timeliness of such a waiver. The validity of such a waiver is more likely to be questioned where a lengthy period of time has passed since receiving the consent, or the patient's personal situation has changed so markedly that there are grounds to suggest their views may have changed. Reasonable steps must be taken to ensure that the waiver remains current.



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

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

#### Example

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



#### Further guidance:

- [NSW Health Consent to Medical and Healthcare Treatment Manual](#)
- [NSW Health Policy Directive Domestic Violence – Identifying and Responding \(PD2006\\_084\)](#)
- [Integrated Prevention and Response to Violence, Abuse and Neglect Framework \(PD2019\\_041\)](#)

#### 7.4.1.4 Where the information is collected from a third party

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

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

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



#### Further guidance:

- NSW Privacy Commissioner [Statutory guidelines on collection of health information from a third party](#)

#### 7.4.2 What information do individuals need to be told?

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

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



#### Further guidance:

- [NSW Health Privacy Leaflet for Patients](#)

#### 7.4.3 When should individuals be told?

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

If it is not practicable to inform the individual at the time the information is collected, the health service should do what it reasonably can to inform the individual as soon as practicable after that time.

#### 7.4.4 How should individuals be told?

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

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

- [NSW Health Privacy Leaflet for Patients](#) (see Section 7.4.5) to be made available to all patients
- Verbal reinforcement or explanation of [NSW Health Privacy Leaflet for Patients](#) (see Section 7.4.5) to be made available to all patients where necessary
- Privacy poster (see Section 7.4.6) and notices displayed on counters and other public areas of health services. An electronic NSW Health privacy poster is available from the Ministry of Health, which can be displayed on work computers and other public screens.
- Information included on admission forms, correspondence, and emails
- Information provided on the health service's website.

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

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

## 7.4.5 Privacy Leaflet for Patients

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

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

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

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

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

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

A contact list for NSW Health Privacy Contact Officers is available via the [NSW Health privacy webpage](#).

The [NSW Health Privacy Leaflet for Patients](#) is available in 29 community languages via the NSW Health Privacy website, or via the [Multicultural Health Communication Service website](#).

### 7.4.5.1 Privacy Leaflet for Patients – Distribution

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

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

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



#### Further guidance:

- Section 7.4.2 What information do individuals need to be told?
- Section 11 Using & disclosing personal health information (HPPs 10 & 11)
- [NSW Health Privacy Leaflet for Patients](#)

### 7.4.6 Privacy poster

The NSW Health Privacy Poster should be displayed in public areas, such as in Emergency Department waiting rooms, Outpatient and Community Health waiting rooms. In addition, the Privacy Poster should be displayed, where appropriate, in wards, corridors, at information points, concierge and nurse stations. An electronic NSW Health privacy poster is available from the Ministry of Health which can be displayed on work computers and other public screens.

Please contact the Privacy Contact Officer for your health service for copies of the hard copy or electronic Privacy Poster.

### 7.4.7 Youth-friendly privacy resources

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

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

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

The Youth-friendly confidentiality resources are available via:

- NSW Health 'Better Health Centre' via [NSLHD-BHC@health.nsw.gov.au](mailto:NSLHD-BHC@health.nsw.gov.au)
- [NSW Health Kids and Families website](#)



#### *Further guidance:*

- Section 5.5.2 Minors
- [Youth Health Framework 2017-24 \(PD2017\\_019\)](#)

# 8 Anonymity (HPP 13)

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

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

In some circumstances, such as where a person may be at serious risk of harm, the patient (or police) may request anonymity in a hospital setting, so the patient cannot be located. In these circumstances the use of an alias, or 'disguised identity' is usually a more appropriate approach, given the duty of care owed to the patient and clinical safety needs of the patient. (See Section 8.3 Use of alias or 'disguised identity'.) The health record can then revert to the patient's true identity, at the time of the patient's discharge or other relevant period during which the alias identity is required.

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

## 8.1 When providing a service anonymously may be impracticable

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

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

## 8.2 When providing a service anonymously may be unlawful

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

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

## 8.3 Use of alias or 'disguised identity'

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

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

In this context, the term 'alias' means the same as 'disguised,' 'restricted' or 'masked' identity. Different health services use different terminology and may use different methods to disguise the identity of a patient.

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

- the patient is under witness protection
- the patient is under police guard/ custody
- the patient is a child at risk
- the patient is at risk of domestic violence
- the patient is concerned about potential (unwanted) media attentions or visitors
- the patient has requested an alias
- court or intervention orders apply
- following a valid request from law enforcement agencies

On conclusion of the patient's episode of care, or other relevant period during which the alias identity is required, the name used to refer to the patient will revert to the patient's real name. This does not occur when patients are treated anonymously (see Sections 8.1 and 8.2 above).

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

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

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

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



# 9 Retention, security and protection (HPP 5)

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

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

## 9.1 Retention and disposal of personal health information

HPP 5 operates subject to other lawful requirements. As public sector agencies, health services are subject to the requirements of the [State Records Act 1998](#). That Act has extensive provisions as to the minimum length of time public records must be retained and creates a statutory framework for authorising the disposal of State records and for deciding which records will be retained as State archives.

Disposal is usually authorised through retention and disposal authorities issued by NSW State Archives and Records. Health services should therefore refer to the relevant General Disposal Authorities in determining how long to retain and how to dispose of health records.



### Further guidance:

- [NSW Health Policy Directive \*Health Care Records – Documentation and Management\* \(PD2012\\_069\)](#)
- [NSW Health Electronic Information Security Policy Directive \(PD2020\\_046\)](#)
- [IB2019\\_015: General Retention and Disposal Authority: Patient Records \(GDA 17\) and Administrative Records \(GDA 21\)](#)
- [State Records NSW Destruction of Records Guidelines](#)
- [State Archives and Records General Retention and Disposal Authorities](#)
  - General Disposal Authority No. 11: Audio visual programs and recordings
  - [General Disposal Authority No. 17: Public health services: patient/client records](#)
  - Functional Retention and Disposal FA427: Forensic Medicine

- General Disposal Authority No. 21: Health Services, Public: Administrative Records
- General Authority No. 28: Administrative Records
- General Authority 31: Royal Commissions, Special Commissions of Enquiry
- General Disposal Authority No. 42: Public Health Services: general practice records
- General Disposal Authority No. 44: Health services: state-wide health services, quality assurance, reporting, education, and training
- General Authority 45: Original or source records that have been copied

## 9.2 Security of personal health information

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

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

The appropriate levels of security controls should be determined through a formal risk-based security assessment, such as the [NSW Health's Privacy and Security Assurance Framework \(PSAF\)](#) accessible via SARA.

Health services must ensure that reasonable processes are in place to keep information secure, which will include:

- taking steps to make staff aware of their privacy obligations
- restricting staff access to patient health information to only those employees who need to access it to perform their duties
- informing staff that their actions in accessing patient health information will be monitored and may be subject to audit
- informing staff of the consequences that may follow unauthorised access, use or disclosure of health information
- taking action against employees in respect of unauthorised access, use or disclosure of health information where it considers it appropriate.



#### Further guidance:

- Section 13.3 Linkage of health records (HPP 15)
- Section 16 Electronic health information management systems
- [NSW Health Electronic Information Security Policy Directive \(PD2020\\_046\)](#)
- [NSW Health Policy Directive, Use & Management of Misuse of NSW Health Communications Systems \(PD2009\\_076\)](#)
- [NSW Cyber Security Policy](#)
- Section 6.1.2 Staff Training

## 9.2.1 Hard copy health records

### 9.2.1.1 Storage

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

### 9.2.1.2 Access at patient bedside

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

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

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

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

Staff should take reasonable steps to ensure that it is clear the health records held at the patient's bedside are confidential and should only be accessed when clinical staff are present. Placing a prominent notice on the front of health records held at the patient's bedside is an example of one strategy to manage privacy. For example, the following text may be used:

**CONFIDENTIAL INFORMATION:** *This is a confidential health record. Do not access, read or remove this health record unless you are authorised. Patients, relatives and visitors must speak to a staff member if they wish to view any part of the patient health record.*

### 9.2.1.3 Disposal

Paper records containing personal health information should be disposed of by shredding or pulping, in accordance with the provisions of the [State Records Act 1998](#). Where large volumes of paper are involved, specialised services for the safe disposal of confidential material should be employed, and certificates of disposal obtained from the contractor. Special care should be exercised to ensure that paper records are not lost or misplaced when health service buildings are decommissioned. Paper records should be securely archived or destroyed as part of the decommissioning process.



#### Further guidance:

- Section 9.1 – Retention and disposal of personal health information

## 9.2.2 Images and photography

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

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

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

Collection of photo and video imaging must be relevant to the purpose, accurate, not excessive and not unreasonably intrusive. Staff should ensure that informed consent is obtained from the patient whenever possible.

It is important that the equipment used is appropriate for the purpose, for example, has the necessary level of resolution and quality to meet the clinical purpose. For certain types of services, additional security and personal privacy issues may also arise. For this reason, Health services should adopt local protocols and policies addressing the type of equipment authorised for use in different clinical settings and the storage of images in the health record.

Where practicable, images should be captured on NSW Health equipment and devices.

From time to time, emergency situations may arise where a personal mobile phone or other personal device is used to capture and temporarily store images for clinical purposes, due to an urgent need for diagnosis and treatment. If practicable, the patient should be made aware that a personal device is being used to capture the clinical image. A personal device must never be used to capture intimate images or for forensic photography. The use of personal devices must comply with policies on the protection of children and the [\*NSW Health Code of Conduct \(PD2015\\_049\)\*](#). If a personal device is used to capture images, staff should take particular care to transfer all data from the device to the local health records management system, in accordance with local health records management policy. The image must then be permanently deleted from the personal device and associated storage (for example cloud backups).

The use of personal devices to capture images of patients for non-clinical purposes is generally not permitted.

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

Staff should consult with:

- Health Information Service for assistance with local image management and medico-legal requirements
- Information Technology Department for guidance on local image management, technical and security provisions

- Sexual Assault Service with regards to images of injuries sustained by victims of sexual assault

Additional policies and procedures must be followed for the capture of forensic photography and recordings, and special considerations will also apply to intimate images captured for forensic purposes. A valid, written record of consent must be obtained and recorded.

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

For guidance on the use of images for education, training or conference purposes see:

- Section 9.2.6 Training and presentations
- Section 11.2.5 Management, training or research



#### Further guidance:

- [\*NSW Health Code of Conduct \(PD2015\\_049\)\*](#), Section 4 (social media)
- [\*NSW Health Public Communication Procedures \(PD2017\\_012\)\*](#).
- [\*Australian Medical Association: Clinical images and the use of personal mobile devices.\*](#)
- [\*Responding to Sexual Assault \(adult and child\) Policy and Procedures \(PD2020\\_006\)\*](#).
- [\*Photo and Video Imaging in Cases of Suspected Child Sexual Abuse, Physical Abuse and Neglect \(PD2015\\_047\)\*](#).
- [\*Domestic Violence – Identifying and Responding \(PD2006\\_084\)\*](#)
- [\*Bring Your Own Device and NSW Health Smart Devices Policy Directive \(PD2022\\_011\)\*](#).

### 9.2.3 Computer systems and applications

The [\*NSW Health Policy Directive Electronic Information Security \(PD2020\\_046\)\*](#) supports NSW Health in meeting its obligations for protecting personal health information from unauthorised access, disclosure or other misuse. Staff should also refer to the local security rules for computer systems and

applications, including electronic health information management systems (see Section 16 Electronic health information management systems).

Staff with access to electronic applications, such as an electronic health record, may only access, view, use or disclose health information held the system for purposes directly related to their work. If in doubt, staff should seek advice from a senior manager, local Health Information Service or Privacy Contact Officer. Staff should be provided with the appropriate level of access to physical and electronic health records (i.e., full, partial or no access) in accordance with their role and their work requirements.

### 9.2.3.1 NSW Health devices and approved personal devices

NSW Health staff can use NSW Health owned mobile phones, laptops and other smart devices and/or approved personal devices to access NSW Health information systems. Staff must have appropriate approval to use personal devices. The NSW Health [\*Bring Your Own Device and NSW Health Smart Devices Policy Directive \(PD2022\\_011\)\*](#) establishes the security requirements that must be addressed for staff to be able to use approved personal devices including mobiles, tablets and laptops to access NSW Health systems.



**Further guidance:** :

- [\*Bring Your Own Device and NSW Health Smart Devices Policy Directive \(PD2022\\_011\)\*](#)

### 9.2.3.2 Patient devices and remote patient monitoring

In some clinical circumstances, patients are given electronic devices as part of home care and remote patient monitoring. This might be to manage conditions like diabetes and home dialysis, for example. Staff need to ensure that any personal health information held on these devices is removed before the devices are issued to other patients. Staff also need to ensure that patients understand the security requirements of the devices and how the security of their health information is managed. If suppliers of patient devices are to be given access to personal or health information of users of devices, patients must be informed about this access to their information and its purpose.

### 9.2.3.3 Collaboration tools

There is increasing use of online collaboration tools by NSW Health staff to share information. Collaboration tools are used for documentation management and for holding online meetings.

Privacy and security risks arise when health information or personal information is shared using these tools.

Collaboration tools supported for use by NSW Health must have undergone the eHealth NSW [\*Privacy and Security Assurance Framework \(PSAF\)\*](#) process. Staff should comply with the eHealth [\*Guidelines on ICT Collaboration Platforms\*](#) which outline the specific collaboration platforms which are supported for use by NSW Health staff and the recommended uses of each platform.

Health organisations should provide staff guidance on restrictions to the types of information to be shared using collaboration tools. Staff should ensure appropriate access controls are in place so that access to health information held in collaboration tools is restricted to those who require access for their work role.

Due to privacy risks, generally online meetings which involve discussion of patient health information should not be recorded unless there is a strong justification e.g. conducting a formal investigation where a recording is made because it may be required as evidence in legal proceedings (see Section 15.11A). If a recording is made, consideration must be given as to whether to retain the recording as a State Record under the [\*State Records Act 1998\*](#). Local business rules should be developed for the management, retention and secure disposal of such recordings.



**Further guidance:**

- eHealth NSW, [\*NSW Health ICT Collaboration Platforms Guidelines \(HD21/9531\)\*](#)
- eHealth NSW, [\*NSW Health Video Conferencing Platforms Guidelines \(HD21/35944\)\*](#)
- NSW Health [\*Bring Your Own Device and NSW Health Smart Devices Policy Directive \(PD2022\\_011\)\*](#)
- Section 9.2.2 Images and photography
- Section 15.11A Recording online meetings

### 9.2.3.4 Disposal of digital health information

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

NSW Health organisations must comply with eHealth NSW guidance on e-waste disposal, including with respect to engaging approved providers of e-waste disposal and destruction services.

Personal health information must be deleted from Health organisations' hardware (including devices,



computer hard drives, printers, and photocopiers) and supplier storage devices before being recycled, disposed of, used by another employee, or sent back to a leasing agent or contractor.

This includes any devices used to capture images or other patient data (for example, memory cards in cameras/video cameras/phones/tablets).

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

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



#### **Further guidance:**

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

### **9.2.4 Safeguards when delivering and transmitting information**

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

If the use or disclosure is authorised, the following minimum standards should be applied when sending the information.

Requirements needed to maintain secure delivery will vary depending on the information's medium of transmission.

#### **9.2.4.1 Telephone**

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

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

health service may be used, if applicable and appropriate in the circumstances.

#### **9.2.4.2 Use of text messages (SMS/MMS) to communicate with patients**

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

Where patients agree to being sent their test results by SMS, health services are increasingly using SMS as a standard practice for communication with patients, including, for example, some sexual health services and for delivery of COVID-19 results (with patient consent).

Even where SMS communication is standard administrative practice, patients should, if they request it, be given other options to receive information or results and care should be taken to avoid any sensitive descriptors, where possible. The SMSs should be as generic as possible.

In some health services it may be appropriate to use SMS for specific clinical purposes. However, this would need to be supported by sound governance systems to ensure patient care is not compromised and proper records are maintained. Additionally, any use of SMS should be conducted with the patient's consent.

Patients may also use text messages to provide health information to clinicians (e.g., blood glucose scores, wound care) for review. Clinicians need to ensure any such health information received from patients in this way is transferred into the patient's medical record as it forms part of the patient's clinical management and is deleted from the clinician's device as soon as practicable.

#### **9.2.4.3 Use of messaging tools to share information with other clinicians**

Staff must only use instant messaging tools approved by the eHealth NSW [\*Privacy and Security Assurance Framework \(PSAF\)\*](#) process.

Health organisations should have local rules on minimising security and privacy risks when using approved messaging tools. If messaging tools are used for the purpose of clinical care, health information relevant to the patient's care must be saved onto the patient's health record and deleted from the device and the instant messaging tool.

In certain circumstances, the record of an exchange of information using messaging tools may be considered to be a State Record under the [\*State Records Act 1998\*](#). Local business rules should



address the management, retention and secure disposal of such records.



#### Further guidance:

- NSW Health [Bring Your Own Device and NSW Health Smart Devices Policy Directive \(PD2022\\_011\)](#)

#### 9.2.4.4 Facsimile

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

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

#### 9.2.4.5 Mail

Some patient information is still sent by mail. The following steps are recommended when sending personal health information via mail:

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

#### 9.2.4.6 Transmission of electronic documents (discharge referrals / summaries)

NSW Health has a number of systems (e.g. HealtheNet) which deliver electronic documents (e.g. discharge summaries and referrals (eDRS)) to external health care providers (such as general practitioners,

specialists and allied health care providers), as part of providing ongoing care in the community.

These systems rely on the accuracy and currency of the providers nominated by patients to receive information. Given this, health staff should:

- check the accuracy of patient information updated in auto populated fields (including current address, GP, authorised representative) at each admission
- have processes in place to manage a consistent and single source of general practitioner, specialist, and other community providers' details at the health service level.
- record accurate and complete community provider details.
- have processes in place to authenticate and monitor the accuracy of service provider details and to update this data on a regular and frequent basis.
- provide all relevant staff with education and training on their data collection responsibilities and the importance of policies and procedures in relation to provider details.
- include an appropriate privacy notice in each transmission message. For example, the message could be marked as follows:  
**CONFIDENTIAL:** *If you are not the intended recipient you must not use, disclose, copy or distribute this communication. If you believe you have received this message in error, please ensure you delete it and notify the sender.*

#### 9.2.4.7 Email within NSW Health

Email within NSW Health should comply with the [NSW Health ICT Collaboration Platforms Guidelines \(HD21/9531\)](#) in relation to recommended uses of Microsoft Outlook. Staff must also comply with local health information policies when sending personal health information via email.

For the highest level of security protection, it is strongly recommended that staff use secure file transfer tools or approved secure collaboration tools whenever it is practicable to do so, when sending personal health information.

If use of such tools is not practicable, further security measures should be considered when using email. For example:

- Use of email should not replace the recording of personal health information in electronic or paper health care records. However, an email containing health information used for the purposes of providing treatment or ongoing healthcare is likely to constitute a health record, in which case the email should be incorporated into the patient's

health record (i.e. transcribed as 'email advice received,' scanned or printed and filed)

- The subject title of emails which include personal health information should include 'OFFICIAL: Sensitive – Health Information'
- Emails which include personal health information must include patient identifiers to ensure that the content of the email, or the email itself, is filed against the correct patient. The national standard for patient identification requires that the following details be provided in all circumstances when referring to a patient: patient's name, sex, date of birth, and Medical Record Number (MRN)
- As with all use of personal health information, only include health information which you know to be required for the purpose of email communication
- Take care not to inadvertently copy unintended recipients when sending the email.
- Make use of the blind copy (BCC) option when sending group emails to patients, to ensure that email addresses containing identifying information (that may identify a patient) are not unintentionally disclosed to other patients. Consider use of other tools, such as approved secure SMS messaging apps, to securely send group messages
- Exercise caution when using the 'Reply All' function. Always check that it is appropriate for your email's content to be provided to recipients
- Emails and attachments containing personal health information should be filed, as appropriate in the eMR or other filing system and then deleted from the inbox (and trash emptied) within 30 days
- When sending health information via email internally or externally, staff may want to consider reminding recipients to delete the information from their inboxes as soon as it is appropriately filed, for example:

*'Information relating to [XXX patient] is provided [for X purposes]. To ensure the security of this health information, I would be grateful if you would delete (and trash empty) this email from your mailbox as soon as the content is appropriately filed.'*

*You are required, in accordance with privacy laws, to keep this information confidential and to only use it for the purpose of responding to the current [complaint/claim/ investigation].'*



#### Further guidance:

- On health service activities which are considered to be directly related to patient care, see Section 11.2.1 Directly related purpose.
- [DCS-2020-07 NSW Government Information Classification, Labelling and Handling Guidelines](#)
- [eHealth NSW Information Security Services, Advice when emailing personal information and/or health information](#)
- [eHealth NSW, NSW Health ICT Collaboration Platforms Guidelines \(HD21/9531\)](#)

#### 9.2.4.8 Email external to NSW Health

Use of email for the transmission of personal health information to destinations external to NSW Health (i.e. any email not ending in @health.nsw.gov.au) is not considered secure. For the highest level of security protection, it is strongly recommended that staff use secure file transfer tools or approved secure collaboration tools whenever it is practicable to do so, when sending personal health information. If it is not practicable to use such tools, emails should be password-protected or encrypted prior to transmission in accordance with local health service policy.

There may be limited circumstances when use of unencrypted emails to transmit health information outside of NSW Health is acceptable, despite the security risk. Such circumstances include where it is necessary to use email to avoid a negative impact on patient care such as clinical emergencies, or communications with patients or external clinical services that do not include significant amounts of health information. These decisions need to strike an appropriate balance between efficiency, patient care requirements and privacy obligations.

When sending emails external to NSW Health, the minimum amount of personal health information should be disclosed as required for the purpose. Care should always be taken to avoid including patient details in the email subject title or text, where possible. Double check that the email address is correct. If practicable, request that the recipient provides you with their email address by emailing you first.

In addition, consideration should be given to whether any email correspondence should be captured and stored in a patient medical record.

Where password protection of emails is used, the password should not be sent via email to the recipient. The recipient should be notified of the password by telephone or text message.



#### Further guidance:

- Refer to the recommended security measures for sending emails set out in Section 9.2.4.7. They are also relevant for sending external emails.
- Consult your ICT team or Privacy Contact Officer, or consult eHealth NSW, if you need options to securely transfer personal health information.
- eHealth NSW, [\*NSW Health ICT Collaboration Platforms Guidelines \(HD21/9531\)\*](#)
- eHealth NSW Information Security Services, [\*Advice when emailing personal information and/or health information\*](#)

#### 9.2.4.9 Secure file transfer (SFT)

When sharing information or files over the internet, there is a risk of loss or exposure to cyber-attacks depending on the file transfer process used. Some current sharing methods such as email, file transfer protocol, and external storage devices pose a security risk. Secure File Transfer (SFT) provides a means to securely send and exchange file attachments of any size. All communications are secured using industry standard encryption and protected from unauthorised access, as each recipient must be authenticated and securely log in to use the service.

eHealth's approved SFT service for all NSW health organisations is available on the [eHealth NSW intranet](#).

SFT is particularly useful for large, sensitive documents or files. Access to the data is time limited to improve security.

SFT is also recommended for internal uses including the transfer of attachments containing unit record data or otherwise large volumes of personal health information between NSW Health organisations.

Additionally, many IT systems in use by NSW Health organisations have enhanced security measures that mean document storage, file sharing and editing can be better secured (including Kiteworks and secure functionalities in SharePoint and OneDrive).

Each entity should develop its own procedures for the secure transmission of patient information with internal and external recipients, utilising the secure storage and transmission functionalities of IT systems.



#### Further guidance:

- [\*NSW Health Electronic Information Security Policy Directive \(PD2020\\_046\)\*](#)
- [\*NSW Health Policy Directive, Use & Management of Misuse of NSW Health Communications Systems \(PD2009\\_076\)\*](#)
- eHealth NSW Information Security Services, [\*Advice when emailing personal information and/or health information\*](#)

#### 9.2.4.10 USB sticks and other portable media

The storage or transfer of personal health information on portable media such as USB or other applications should generally be limited to NSW Health-owned media which encrypts the data stored and should only be on a temporary needs basis. Reasonable steps must be taken when storing or transferring information in this way to reduce the risk of unauthorised access to the information, such as developing unique password entry into documents and /or encrypting the USB drive.

#### 9.2.5 Printing and copying

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

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

#### 9.2.6 Training and presentations

The anonymity of patients should be maintained during case presentations, demonstrations, research activities and in presentations or discussions at seminars and conferences. Where possible, fictitious data should be used.

Consideration should be given to de-identification of photos, slides, and other visual aids. Identifying features such as eyes, birthmarks, tattoos, and jewelry are required to be redacted. When identification of individuals is necessary or unavoidable, the consent of the patient or an authorised representative of the patient should be obtained.

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



**Further guidance:**

- Section 11.2.5 Management, training, or research
- [NSW Privacy Commissioner's Statutory Guidelines on Training](#)

## 9.2.7 Conversations

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

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



**Further guidance:**

- Section 15.11A Recording online meetings

## 9.2.8 Visibility of computer screens

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

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



**Further guidance:** :

- Privacy training modules available from [HETI](#) including Cyber S.A.F.E. modules and Cyber Fundamentals e-module

## 9.2.9 Whiteboards and patient journey boards in public view

It is common practice to display limited personal health information about patients on wards using a whiteboard, electronic board, patient journey board, and so on. The purpose for displaying patient information in this way is to enable staff to deliver safe and efficient clinical care for patients. Displaying limited personal health information in this way enables fast and effective communication between staff.

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

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



**Further guidance:**

- [Electronic Patient Journey Boards: Balancing Clinical Benefit and Privacy Obligations](#)

# 10 Accuracy (HPP 9)

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

To ensure that the health record is accurate and complete:

- information should be recorded at the time of consultation or procedure, as soon as it becomes available, or as soon as it is practicable to do so
- entries should generally be made by those collecting the information or present when the information was collected
- this must also be documented in the patient's health record
- each entry should contain a clear and legible notation of the health care provider's name and designation, the date and time, and should be signed by the health care provider
- accuracy of patient details should be checked by administrative staff at each presentation, e.g., name, date of birth, address, GP details, etc., including information updated in auto populated fields
- alterations or deletions should not be made. Original incorrect entries should not be erased but lined through so the original entry remains readable, and such action should be explained, signed, and dated
- electronic medical record entries should be kept in read-only format; any access to alter or delete entries should be controlled and regularly audited
- patients should be notified of amendments to their health record where appropriate
- the treating health practitioner should periodically review the health record for correctness
- there should be an audit trail for electronic health records.



## Further guidance:

- Section 16 Electronic health information management systems
- NSW Health Policy Directive [\*Health Care Records – Documentation and Management \(PD2012\\_069\)\*](#)
- NSW Health Policy Directive [\*Client Registration Policy \(PD2007\\_094\)\*](#)
- NSW Health Policy Directive [\*NSW Health Admission Policy \(PD2017\\_015\)\*](#)



# 11 Using and disclosing personal health information (HPPs 10 & 11)

In general terms, a ‘use’ of personal health information refers to the communication or handling of information within NSW Health.

NSW Health is a single agency for the purposes of the *Health Privacy Principles*. Therefore, sharing health information between health services is considered a ‘use’ (see Section 3.2 NSW Health agencies to be treated as a single agency).

A ‘disclosure’ refers to the communication or transfer of information *outside* NSW Health. A disclosure can occur by:

- giving a copy of the information to another organisation or individual
- allowing another organisation or individual to access or view the information
- giving out summaries or communicating the information to another individual or entity in any other way.

As part of good clinical practice, patients should be included in decisions regarding the use and disclosure of their personal health information. This may occur, for example, at the time of collecting consent for treatment, or during consultation with the patient.

Use and disclosure are treated together as privacy law generally imposes the same conditions on both activities. An exception is that the disclosure provisions also allow disclosure on compassionate grounds (see Section 11.2.10), which does not apply to ‘use’.

There are three broad categories of use and disclosure authorised under privacy law:

- where information is used or disclosed for the ‘primary purpose’ for which it is collected, OR
- where information is used or disclosed for another ‘secondary purpose’, and one of the criteria listed in the HPPs applies, OR
- where the use or disclosure of the information is lawfully authorised.

Activities which fall outside of these three categories are not permitted without patient consent unless a Public Interest Direction is obtained pursuant to section 62 of the [Health Records and Information Privacy Act 2002](#).

**NSW Health staff may only view, access, use and disclose personal health information when it is necessary for them to do so to carry out their work duties or for other authorised purposes.**

Section 15, Common privacy issues, provides guidance on how to address some common requests for use and disclosure of patient health information including requests for media access (see Section 15.7) and fundraising (see Section 15.8).

Staff must not access health information of family, friends or others for personal purposes unrelated to their work. If in doubt, staff should seek advice from a line manager and/or senior manager, local Health Information Service, or local Privacy Contact Officer.

## 11.1 Use and disclosure for the ‘primary purpose’

A health service may use or disclose information it has collected for the purpose for which it was collected. The primary purpose will generally be the ‘dominant purpose’ for which the information was collected. Most often in the health system, the purpose for collecting personal health information will be to provide a health service.

### Examples

A person is admitted to hospital for exploratory surgery for suspected cancer. The ‘primary purpose’ for collecting their information at admission is to provide this service and will allow disclosure to those involved in the surgery, and others involved in providing the service, for example, health care providers including nursing staff, anaesthetists and pathologists.

Some months after the patient’s discharge, the oncology unit proposes to conduct a fundraising drive, and proposes to use the information from health records to target recent admissions. As fundraising was not the ‘primary purpose’ for which this information was collected and is not an authorised secondary purpose under the privacy laws, the oncology unit can only use the personal health information for this purpose if patient consent for contact was obtained at the time of collection of their personal health information. Consent is required prior to using patient information for fundraising purposes.

## 11.2 Use and disclosure for a 'secondary purpose'

The health service may also use or disclose information for another 'secondary purpose' if this is covered by one of the exemptions listed in HPPs 10(1) and 11(1). The secondary purposes listed under HPPs 10 and 11 are:

- use or disclosure for a directly related purpose, which would be 'reasonably expected' by the individual (see Section 11.2.1)
- use or disclosure to which the individual has consented (see Section 11.2.2)
- use or disclosure to prevent a serious threat to health or welfare (see Section 11.2.3)
- use or disclosure to assist in the stage of emergency (see Section 11.2.4)
- use or disclosure for management, training or research purposes (see Section 11.2.5)
- use or disclosure to assist in finding a missing person (see Section 11.2.6)
- use or disclosure as part of investigating and reporting wrong conduct (see Section 11.2.7)
- use or disclosure to or by a law enforcement agency or investigative agency (see Sections 11.2.8 and 11.2.9)
- disclosure made on compassionate grounds (see Section 11.2.10).

The information may also be used or disclosed if there is a 'lawful authorisation' to do so (see Section 11.3).

### 11.2.1 Directly related purpose HPP 10(1)(b) & 11(1)(b)

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

All patients must be provided with the 'Privacy Leaflet for Patients'. NSW Health staff should be aware that some patients will not share the same general expectations as other patients for a variety of reasons, for example, if they have previously received health care in a different country, or if they are particularly sensitive about aspects of their health care. Wherever practicable, NSW Health staff should make considered and respectful efforts as are reasonable in the circumstances to explain to patients how patient information is generally used and disclosed.

Sharing of health information for a directly related health care purpose often arises in the health system, particularly in relation to sharing information with other health care providers (see Section 15.1 Third party health care providers).

#### 11.2.1.1 'Directly related purpose'

This secondary purpose recognises there are activities that are necessary for health services to perform as part of their day-to-day operations, such as provision of ongoing care, billing and the following up of test results, which may not fall within the primary purpose for which the information was collected.

What is a directly related purpose will vary depending on the circumstances. There are however some common examples of what is likely to fall within the 'directly related purpose' exemption. These include:

- using the information to provide ongoing care to patients

#### Example

An antenatal unit from another hospital is requesting a copy of a patient's health records relating to her previous pregnancy. As information relating to a previous pregnancy is likely to be relevant to the current pregnancy, it can be provided on the basis of ongoing care. It would also be expected that as a matter of good clinical practice the hospital requesting the information would have discussed this with the patient prior to making the request.

- disclosing health information to the patient's nominated GP, other treating health services, hospitals or medical specialists involved in the care and treatment of a patient
- providing relevant health information to carers to assist with care for the patient
- using or disclosing NDIS documents, such as NDIS Plans, for the purposes of the [\*National Disability Insurance Scheme Act 2013\*](#), for example, to provide reasonable and necessary supports for NDIS participants, which may include sharing NDIS documents with third parties to help them provide reasonable and necessary supports for NDIS participants. If the information sought is unrelated to health care or is regarding financial entitlements, patient consent should be sought – see Section 4.1.11 NDIS. Contact your organisation's Privacy Contact Officer for further information.
- sending reminders to a patient where the person receives a service on a regular basis or requires a follow up service

- administrative activities associated with providing, following up on or receiving payment for the service or product and follow up on an overdue payment (including disclosures to a debt collector). The information provided should be limited to what is relevant to the claim
- using the information to manage the provision of the service or product
- contacting a patient for feedback on the services received for the purpose of evaluation and improvement of services
- receiving and using patient information from approved remote patient monitoring platforms for the purpose of home monitoring
- providing relevant patient information to accredited hospital chaplains and pastoral care workers providing spiritual and pastoral care in accordance with the [Health Records and Information Privacy Regulation 2022](#) (see Section 11.2.11 Chaplaincy services)
- sharing relevant patient information with students and other staff for training purposes (see Section 11.2.5 and the [Statutory Guidelines](#))
- maintaining lists of patient names for patient care and safety purposes, for example, maintaining patient lists for fire evacuation for use by the fire brigade in event of an emergency
- using and disclosing patient information for purposes relating to the operation of the health service and treatment of patients, including funding, planning, safety and quality improvement activities
- using information for quality assurance or clinical audit activities carried out by the health service. This includes monitoring, evaluating or auditing the provision of the particular product or service which the health service has provided or is providing to patients (including activities undertaken to comply with the [NSW Patient Safety and Clinical Quality Program](#))
- disclosing information to an auditor or quality assessor for the purposes of monitoring, evaluating or auditing the provision of a particular product or service the health service has provided or is providing to the person (as long as the individual reviewing the health records is bound by privacy legislation or a professional code of ethics)
- some management and research activities may be considered a purpose directly related to health service delivery (see Section 11.2.5 Management, training or research)
- using and disclosing the information to investigate complaints about care provided by the health service or patient safety

- using and disclosing information to enable follow-up of complaints about the service or a product, or recalls of a product
- using or disclosing relevant information to claims managers and associated persons while managing a complaint, legal action or claim brought against the health service (See Section 12.5.4 Access by staff responding to a complaint, claim or investigation).

Staff with access to electronic health records may only access, view and use the system for authorised purposes. This means NSW Health staff may only view, access, use and disclose personal health information when it is necessary for them to do so to carry out their work duties, whether that be patient care or other directly related work duties that require access to personal and health information, for example, patient billing or human resource management. If in doubt about their obligations, staff should seek advice from a senior manager, local Health Information Manager or Privacy Contact Officer.

#### 11.2.1.2 'Reasonable expectation'

While the definition of directly related purpose is quite broad, the purpose must also be within the 'reasonable expectation' of the patient. This means that the purpose is closely related to the care and treatment **and/or** that the use or disclosure was communicated when the information was collected. The information given to the patient by the health service when the patient presents for care thus becomes important (the [Privacy Leaflet for Patients](#) and other information provided before or during clinical care).

Where it is made clear to the patient as part of the process of collecting their health information that their information may be used or disclosed for these purposes, then there is a more persuasive argument that the patient would 'reasonably expect' the health service to use or disclose their information in these ways.



#### Further guidance:

- Section 7 – Collecting personal health information (HPPS 1-4), sets out the types of information that needs to be provided and the ways it may be given.
- [Privacy Leaflet for Patients](#)

### 11.2.1.3 Outside a patient's 'reasonable expectation'

In rare circumstances, a patient may make a special request that their personal health information is not used or disclosed for purposes described in this Manual as directly related to the patient's health care (see Section 11.2.1.1 'Directly related purpose').

When health service staff receive such a request, the professional judgement of local health service staff will be required to resolve such requests on a case-by-case basis. To assist staff in exercising judgement, the following guidance is provided:

- A senior clinician should consider whether it is reasonable and practicable to meet the patient's request without putting the patient, staff member or any other person at risk of harm. Wherever it is possible to meet the patient's request, reasonable steps should be taken to comply with the request, and this should be documented in the patient's health record.
- Where it is not possible to comply with a patient's special request, a senior clinician (and other health service staff as necessary) should discuss with the patient:
  - a. the reasons for the patient's concerns about sharing the information
  - b. the reasons why there is a need to share information with all health service staff involved in their care
  - c. the obligations all staff have under privacy law to ensure all personal health information is kept confidential
  - d. the consequences for the patient's health care if personal health information is not shared. This conversation should also be documented in the patient's file.

If the patient remains of the view that they wish information to be withheld and it is the opinion of the treating health practitioner that sharing the information is essential to provide the health service in a safe or appropriate manner, the question then becomes one of whether the patient is prepared to consent to the treatment itself.

The service provider should explain this to the patient and that the facility is unable to provide health services to the patient given this effective refusal. Where appropriate, the facility may wish to offer to refer the patient to another facility or suggest that the patient considers seeking services from another facility.

It is anticipated that the occasions where a service provider will be required to consider the matter as a refusal of medical treatment will be extremely rare.

Staff should work with the patient to resolve the issues and should also contact the Privacy Contact Officer for their health service to liaise with the patient and to participate in resolving such matters.

## 11.2.2 Consent

### HPP 10 & 11(1)(a)

This section is to be read in conjunction with Section 5.4 Consent.

#### 11.2.2.1 Where a third party seeks access

A patient can consent to or authorise any third party, such as a family member, interpreter, health practitioner (not involved in their ongoing care), legal representative, employer or insurer to have access to their health record.

Where health information is being used or disclosed on the basis of consent, consent must be provided by the patient prior to a third-party gaining access to a patient's health information.

Where the patient lacks the capacity to consent, the patient's authorised representative may consent on behalf of the patient (see Section 5.6 Authorised representative).

Where an immediate family member is unable to gain consent from the patient or the patient's authorised representative, for example, in circumstances of family dispute or estrangement, the health service may consider providing the family member with access to limited health information on compassionate grounds, see Section 11.2.10.

Where the patient is deceased, an immediate family member may be provided with access to relevant health records on compassionate grounds (see Section 11.2.10 Disclosure on compassionate grounds) or otherwise via a GIPA application.

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

#### 11.2.2.2 Procedures to follow to ensure the validity of the consent

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

A scanned copy, photocopy or photograph of the original consent document can be accepted when provided by the patient, third parties (such as the patient's legal representative or insurer) and other government agencies.



Where a patient's legal representative or insurer has electronic signing technology this may also be acceptable provided reasonable checks have been made to ensure the legal representative or insurer are verified.

The consent should contain:

- full name of patient
- date of birth
- contact details (current address, telephone number, email address)
- date of written consent (see Section 5.4.1 Elements of consent)
- details of the records or information sought, including range of dates for health treatment
- name of person being authorised and their relationship to the patient
- the purpose for which the information is requested (where relevant).

These requirements are to ensure both the patient and their health records are accurately identified, and to ensure only relevant information is released.

If the health service has reasonable grounds for concern regarding the validity or authenticity of the consent, it should contact the third party and/or patient directly for clarification.

The precise authority of the person requesting access and the nature of that access should be checked to ensure that only relevant material is released. Sometimes a health record will include information about people other than the patient. Health records should be carefully reviewed before release to check for and remove any third-party information in order to avoid a breach of privacy of the third party.

Where there are domestic and family violence concerns, care is needed to ensure the patient's consent is freely given and not pressured or coerced by the identified or suspected perpetrator or others acting on behalf of the perpetrator. Health workers should consult with a Senior Manager, Violence, Abuse, Neglect (VAN) Manager and/or VAN service representative as appropriate.



#### **Further guidance:**

- [\*Domestic Violence – Identifying and Responding \(PD2006\\_084\)\*](#)

Where the request is made for information related to an insurance or compensation claim, a scan or photocopy of the insurance application or

compensation claim form signed and dated by the patient, containing the patient's consent to disclosure, is sufficient authority for the release of relevant health records. It will normally be sufficient for the health service to provide a medical report or summary of injuries for such claims to be processed. If further information is requested, only relevant sections of the patient's health record may be provided.



#### **Further guidance:**

- Section 12.6 Obtain proof of identity
- Section 15.6.3 Patient's Insurer

#### **11.2.2.4 Conditions of access**

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

Confidential patient information must be transmitted securely. For further guidance, refer to information security measures set out in Section 9.2.4.

#### **11.2.2.5 Fees and charges**

Where the person requests copies of a health record, the fees and charges may be required as set out in the relevant NSW Health policy and information bulletin.

The above requirements for consent and conditions of access also apply where the applicant is the patient's legal representative.



#### **Further guidance:**

- Section 5.4 Consent
- Section 12 Patient access and amendment (HPPs 6, 7 & 8)
- [\*Health Records and Medical/Clinical Reports – Charging Policy \(PD2006\\_050\)\*](#)
- [\*Health Records and Medical/Clinical Reports – Rates \(IB2019\\_036\)\*](#)

#### **11.2.2.6 Where the health service seeks to use or disclose**

The proposed use or disclosure may also be initiated by the health service. This may be particularly relevant where the use or disclosure of the information is not a 'directly related purpose'. In such cases, the health service should:



- consider whether the patient has adequate capacity to give consent (see Section 5.4 Consent)
- address the elements of consent outlined in Section 5.4.1 Elements of consent
- make a written record of the consent, either through a written consent form signed by the patient, or by a contemporaneous note of a verbal consent recorded in the patient's health record.

In deciding whether to obtain a written or oral consent from the patient, the following factors should be considered:

- A written consent is the strongest evidence that the patient has given their consent. Written consent is required if there are many or complex issues the patient needs to consider before consenting. Consent would normally be obtained at admission, on commencement of the therapeutic relationship.
- Written consent should also be obtained where the information is proposed to be used or disclosed for a purpose unrelated to the reason for its collection, for example, using a 'good news' story in a hospital newsletter, or for fundraising (see Section 15.8 Fundraising).
- Written consent is not required for day-to-day disclosures relating to ongoing care and treatment, or actions covered by an existing written consent, or where it is otherwise allowed under the *Health Privacy Principles*.

### 11.2.3 Uses and disclosures regarding threats to health and safety, and public health HPP 10&11(1)(c)

A health service may use or disclose personal health information if there are reasonable grounds for believing that this is necessary to lessen or prevent:

- a **serious and imminent threat** to the life, health or safety of the individual or another person, or
- a serious threat to **public health or public safety**.

#### 11.2.3.1 General guidelines

Health staff should be aware that these situations are unlikely to arise in day-to-day case management and so disclosure on this basis will be a relatively uncommon occurrence.

In circumstances where a health practitioner considers that a patient represents a risk to themselves or others, they should carefully assess the level of risk before acting. It is advisable to discuss the situation with an appropriate manager, senior health practitioner or colleague before acting (as is practical and time permitting).

### Examples

A patient of a community health service arrives in an agitated state, making threats against a close family member over a custody dispute. The patient has a history of violence and faced previous assault charges over the same matter. Staff would have reasonable grounds to believe the relative was at serious risk, and so could disclose the information to address this risk.

A Public Health Unit which is investigating and monitoring confirmed or suspected cases of meningococcal infection on a cruise ship which has now left NSW but will be stopping at another Australian port shortly. The Unit would be entitled to share the information with relevant authorities to ensure the serious public health risk is properly addressed as soon as possible.



#### Further guidance:

- [\*Domestic Violence – Identifying and Responding \(PD2006\\_084\)\*](#)

#### 11.2.3.2 Where staff may be at risk

Sharing of information about a patient's violent behaviour is permitted when the patient is referred or transferred within or between facilities (including community health services, aged care facilities and other similar facilities), and when the patient poses a threat to themselves or any individual including staff, or to public health or public safety. Key principles for managing violent behaviour are:

- Privacy obligations must be balanced with health service's obligations to ensure a safe workplace under the [\*Work Health and Safety Act 2011\*](#).
- Relevant patient information should be made available when referring or transferring a patient to ensure patient and staff safety during transfer and to prevent adverse incidents.
- When sharing information about a patient, focus on patient behaviours that may pose a threat or risk, and appropriate patient management strategies.
- A health service must take reasonable steps to ensure the information they share is relevant, accurate, up to date, complete and not misleading.
- Use patient alerts or patient flagging in accordance with [\*'Preventing and Managing Violence in NSW Health Workplace – a Zero Tolerance Approach'\*](#).



#### Further guidance:

- [Preventing and Managing Violence in NSW Health Workplace – a Zero Tolerance Approach'](#) (PD2015\_001)
- [Violence Prevention and Management Training Framework for NSW Health Organisations](#) (PD2017\_043)

**Contact:** [Workplace Relations Branch, NSW Ministry of Health](#)

#### 11.2.3.3 Public Health Act 2010 – Public health risks and public health orders

The [Public Health Act 2010](#) allows for the disclosure of personal health information in limited circumstances between authorities and practitioners where it is suspected on reasonable grounds that a person has a category 4 or 5 condition and the failure to provide the information could place the health of the public at risk. A category 4 or 5 condition includes HIV and TB.

If staff are concerned about a possible health risk relating to HIV or the behaviour of an HIV positive person, they should contact their local HIV coordinator, or the [Centre for Population Health](#), NSW Ministry of Health.



#### Further guidance:

- [Management of people with HIV who risk infecting others](#) (PD2019\_004)

#### 11.2.3.4 Public Health Act 2010 limitations on disclosure of information indicating a person's HIV status

Section 56 of the [Public Health Act 2010](#) provides that a person who, in the course of providing a service, including the conduct of a pathology test, acquires information that another person:

- has been, is to be or is required to be tested for HIV, or
- has, or has had, HIV or AIDS,

must take all reasonable steps to prevent that information from being *disclosed* to any other person.

Section 56 of the [Public Health Act 2010](#) places strict limitations on the release of this information. This information can only be disclosed:

- with the consent of the person concerned, or
- to a person who is involved in the provision of care, treatment or counselling to the person concerned, or

- to the Secretary, if a person has reasonable grounds to suspect that failure to disclose the information would be likely to be a risk to public health, or
- in connection with the administration of the [Public Health Act](#) or the regulations, or
- for the purposes of any legal proceedings arising out of the [Public Health Act](#) or the regulations, or of any report of any such proceedings, or
- in accordance with a requirement imposed under the [Ombudsman Act 1974](#),
- in accordance with the [Mandatory Disease Testing Act 2021](#); or
- in the circumstances prescribed by the regulations.

Information relating to a person's HIV status can be made available to clinical staff if it is relevant to the patient's care for any health condition.

However, health services need to be aware that the requirement to appropriately manage HIV information is still higher than for other types of health information. Most significantly, the exceptions that allow for use and disclosure of other types of health information for secondary purposes, such as research, training, and management, do not apply to HIV information. Staff need to understand that any release or discussion of the HIV information that is not subject to the exemptions could be an unlawful disclosure in breach of the [Public Health Act 2010](#).

The Act provides for a penalty of up to 100 penalty units (\$11,000) or imprisonment for 6 months, or both, for a breach of section 56 without reasonable excuse.



#### Further guidance:

- Section 15.9.6 Managing public health risks
- [Management of People with HIV Who Risk Infecting Others](#) (PD2019\_004)
- [Tuberculosis Management of People Knowingly Placing Others at Risk of Infection](#) (PD2015\_012)
- [Management of health care workers with a blood borne virus and those doing exposure prone procedures](#) (PD2019\_026)
- [Disclosure of Unit Record Data for Research or Management of Health Services](#) (PD2015\_037)
- Section 15.14 – NSW data collections

### 11.2.3.5 Genetic information

The [Health Records and Information Privacy Act 2002](#) allows for the disclosure of genetic information to genetic relatives without patient consent, albeit in very limited circumstances. Genetic relative means a person who is related to an individual by blood, for example, a sibling, parent or descendant of the individual.

Under HPPs 10 & 11(1) (c1) genetic information can be used and disclosed where:

- The disclosure is to a genetic relative of the individual to whom the genetic information relates, and
- It is reasonably believed to be necessary to lessen or prevent a serious threat to the life, health or safety (whether or not the threat is imminent) of that genetic relative, and
- The disclosure is made in accordance with guidelines, if any, issued by the NSW Privacy Commissioner.



#### Further guidance:

- The NSW Information and Privacy Commission [Use and disclosure of genetic information to a patient's genetic relatives: Guidelines for organisations in NSW](#)

The Guidelines encourage health practitioners to take all reasonable steps to obtain consent from the patient (or the patient's authorised representative), and to consult with other experienced health practitioners in the first instance. They also make clear that if a disclosure occurs, only information that is necessary to communicate the risk of harm should be disclosed and, where possible, the patient should not be identified.

The Guidelines may assist an individual and their health practitioner to gain access to relevant records of a deceased genetic relative of the individual where the individual is considered to be at serious risk. Alternatively, where the deceased person is 'an immediate family member', the genetic relative may wish to seek access to the health records on compassionate grounds (see Section 11.2.10 Disclosure on compassionate grounds).

It should be noted that the scope of the Guidelines does not include situations where genetic information presents a serious threat to an unborn child. The patient's consent to disclose genetic information about themselves to a pregnant mother would be required.



#### Further guidance:

- Section 11.2.10 Disclosure on compassionate grounds

### 11.2.4 To assist in a 'stage of emergency'

Exemptions apply to handling of personal information in a 'stage of emergency' as defined in the [State Emergency and Rescue Management Act 1989](#) (HPP 10&11(1)(b1)).

An 'emergency' is defined as an emergency due to actual or imminent occurrence (such as fire, flood, storm, earthquake, explosion, terrorist act, accident, epidemic or warlike action) which

- endangers, or threatens to endanger, the safety or health of persons or animals in the State, or
- destroys or damages, or threatens to destroy or damage, property in the State, or
- causes a failure of, or a significant disruption to, an essential service or infrastructure, being an emergency, which requires a significant and co-ordinated response.

A health service may use or disclose personal health information to assist in a 'stage of an emergency', where the use or disclosure of the information is reasonably necessary to assist in the stage of the emergency, and it is impracticable or unreasonable for the organisation to seek the consent of the individual to whom the information relates.

For the purposes of considering whether a situation amounts to a stage of emergency. Consider the four stages of an emergency set out in the [State Emergency and Rescue Management Act 1989](#):

- **prevention** in relation to an emergency includes the identification of hazards, the assessment of threats to life and property and the taking of measures to reduce potential loss to life or property, and
- **preparation** in relation to an emergency includes arrangements or plans to deal with an emergency or the effects of an emergency, and
- **response** in relation to an emergency includes the process of combating an emergency and of providing immediate relief for persons affected by an emergency, and
- **recovery** in relation to an emergency includes the process of returning an affected community to its proper level of functioning after an emergency.

For example, a hospital or district may consider releasing the names and addresses of all home dialysis patients in a fire risk area to Police or Fire and Rescue NSW when a fire or flood is threatening to endanger those patients. This enables appropriate assistance to be provided to these patients to manage any evacuations and ongoing dialysis in the event of a power outage.

However, under this exemption, if a NSW Health organisation (or another public sector agency) collects, uses or discloses personal information relying on the stage of emergency exemption, it must not hold the information for longer than 18 months, unless extenuating circumstances apply, or consent has been obtained.

This means that the address lists and patient details (described above) provided to Fire and Rescue NSW or Police and prepared by Hospitals or Districts for the sole purpose of the stage of emergency are not to be held for longer than 18-months (after the date of collection). Unless consent is obtained or in extenuating circumstances.



#### **Further guidance:**

- 11.2.8.5 Law enforcement requests in emergency circumstances

### **11.2.5 Management, training or research HPPs 10 & 11 (1) (d), (e) & (f)**

A health service may use or disclose personal health information:

- if it is reasonably necessary for:
  - **funding, management, planning or evaluation** of health services; or
  - **training** the health service's staff members or people who work with the health service; or
  - **research** or the compilation or analysis of statistics in the public interest; AND
- the use or disclosure is in accordance with [\*Statutory Guidelines\*](#) issued by the NSW Privacy Commissioner.

#### **11.2.5.1 When to use this exemption**

Many funding, management, and planning purposes will be a 'directly related purpose' (see Section 11.2.1.1), so you should first check if that exemption applies before considering these exemptions.

For example, data matching of patient information by a health service may be 'directly related' to care if it is required to plan and manage patient care requirements and to ensure staffing, surgery access, bed availability and other management needs are met.

Each of the exemptions for management, training and research has certain preconditions before it can be applied. These are:

#### **The use or disclosure is reasonably necessary for the purpose**

The health service must consider to what degree the personal health information is needed for the

activity. For example, sometimes the activity may be just as effectively undertaken using hypothetical case studies, or simulated situations.

#### **The purpose cannot be served by de-identified information**

If the activity could be undertaken by using/disclosing de-identified information, the provision requires the health service to proceed in that way. This may involve converting 'identifiable' information (information that allows identification of a specific individual) into 'de-identified' information.

De-identified information is information from which identifiers have been permanently removed, or where identifiers have never been included.

Sometimes de-identified information cannot achieve the purpose of the management of health services activity. This could be, for example, where an activity involves linking information about individuals from two or more sources and identified information is needed to correctly link records from each data source.

#### **It is impracticable to seek the person's consent**

The fact that seeking consent is inconvenient or would involve some effort or expense is not of itself sufficient to warrant it to be considered 'impracticable'. Some examples of where it might be impracticable to seek consent include if:

- the age or volume of the information is such that it would be very difficult or even impossible to track down all the individuals involved
- there are no current contact details for the individuals in question and there is insufficient information to get up-to-date contact details
- a complete sample is essential to the integrity and success of the management of health services activity and the activity would not be possible if any persons refused to allow their information to be used.

#### **Reasonable steps have been taken to de-identify the information**

When de-identifying information, you should consider the capacity of the person or organisation receiving the information to re-identify it or link it to identifiable information.

Removing the name and address may not always be enough, particularly if there are unusual features in the case, a small population, or there is a discussion of a rare clinical condition.

Reasonable steps to de-identify might also include removing other features, such as date of birth, ethnic background, and diagnosis that could otherwise allow an individual to be identified in certain circumstances.



Controls and safeguards in the data access environment should be put in place to minimise the risk of re-identification.

### The information will not be published in a generally available publication

A 'generally available publication' is a publication that is generally available to members of the public, either in paper or electronic form.



#### Further guidance:

- [IPC Statutory Guidelines](#)
- [De-Identification Decision-Making Framework, OAIC and the CSIRO.](#)
- [Fact Sheet: de-identification of personal information, Information and Privacy Commission \(IPC\)](#)
- [Privacy issues and the reporting of small numbers, HealthStats NSW](#)
- [Disclosure of unit record data by Local Health Districts for research or contractor services \(PD2018\\_001\)](#)

#### 11.2.5.2 Statutory guidelines

The NSW Privacy Commissioner, Information and Privacy Commission NSW, has issued [Statutory Guidelines](#) that set out conditions imposed on use and disclosure of personal health information for management, research and training.

To view the relevant [Statutory Guidelines](#) go to:

- [Management of health services](#)
- [Training](#)
- [Research](#)

#### Management guidelines

The management guidelines discuss each of the preconditions in detail and draw attention to the relevant 'directly related purpose' which may otherwise apply.

In circumstances where the activities may go beyond a routine management of health services activity and do not appear to come within the 'directly related purpose' exemption, the guidelines provide some further threshold questions to consider before a proposal for the activity must be approved by a Human Research Ethics Committee.

A Human Research Ethics Committee will consider the proposed use or disclosure and assess whether, on balance, it is in the public interest prior to the organisation using or disclosing health information for the purpose of the activity.

#### Research guidelines

The research guidelines are consistent with and mirror the guidelines developed by the NHMRC

under sections 95 and 95A of the [Privacy Act 1988](#) (Cth). Research requiring use or disclosure of personal health information will need to be considered by a Human Research Ethics Committee.

#### Training guidelines

The training guidelines define the circumstances in which personal information can be used in training. The emphasis is on de-identifying the information, except in cases such as student placements and certain staff training where de-identification would defeat the purpose of the training. The guidelines then set requirements for managing such training and the obligations on health services to appropriately protect the information if it is identifiable.

Health organisations seeking to use or disclose health information relying on the 'training exemption' in Health Privacy Principle 10(1)(e) or 11(1)(e) must:

- (a) be reasonably satisfied that the training will make those being trained aware of the privilege that they are being granted; and
- (b) take reasonable steps to ensure that any notes (or other forms of record) containing identifying data and made by persons accessing the information are kept to a minimum.

The guidelines recognise a distinction between training and demonstrations and education programs involving clinical placements as follows:

#### Training and demonstrations

The anonymity of patients should be maintained during case presentations, demonstrations, research activities and at seminars and conferences. Where possible, fictitious data should be used.

Use of photos, slides and other visual aids which allow identification of individuals should not occur unless the material is of critical importance and the consent of the patient has been obtained.

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

A cultural sensitivity warning may be required for Aboriginal and Torres Strait Islander students when clinical records identifying a deceased indigenous person are used for education or training purposes.

#### Clinical placements and students

Students may have access to health records with the approval and under the direction of their supervisor if that access is sought in respect of their education program at the health facility. Access does not include photocopying or transcribing records containing personal health information or taking



such health records off-site. Patients may refuse to have a student participate in their treatment.

Student health professionals must sign a [NSW Health privacy undertaking](#) and must comply with privacy law and all NSW Health policies.



#### Further guidance:

- NSW Privacy Commissioner [Statutory Guidelines on Training](#)
- Section 9.2.6 Training and presentations
- [Disclosure of Unit Record Data for Research or Management of Health Services \(PD2015\\_037\)](#)
- See clinical documentation responsibilities for students in: [Health Care Records – Documentation and Management \(PD2012\\_069\)](#)

### 11.2.6 Finding a missing person

#### HPPs 10(1)(g) & 11(1)(h)

A health service may use or disclose personal health information if the information is to be used by a law enforcement agency to ascertain the whereabouts of a missing person. This exemption only applies if the person has been reported to the police as missing.

#### Example



Police have received a report from a family that their 17-year-old son is missing. The boy has a chronic condition requiring regular treatment in hospital. The police request information from a hospital to ascertain if he has been admitted as a result of failure to take his medication. The hospital would be permitted, but not obliged, to provide this information under this provision.

### 11.2.7 Investigating and reporting wrong conduct

#### HPP 10(1)(h) & 11(1)(i)

A health service may use or disclose personal health information if the health service has reasonable grounds to suspect that there has been or there is the possibility of unlawful activity, unsatisfactory professional conduct or professional misconduct under health registration legislation or conduct by a staff member that may be grounds for disciplinary action. Disciplinary policies should be followed when using or disclosing personal health information for these purposes. Staff and patients should be made generally aware in staff contracts/ patient leaflets that information about them may be subject to such uses and disclosures.

The exemption allows use or disclosure of the information necessary for the health service to investigate or report the conduct in question. It covers but is not limited to information to be provided to:

- the Health Care Complaints Commission
- NSW Health Professional Council or National Board information or
- units of the NSW Ministry of Health which may conduct investigations into breaches of legislation, including the Pharmaceutical Services Unit (NSW Ministry of Health)
- investigative units within NSW Health

#### 11.2.7.1 Public Interest Disclosures

When examining reports of wrong conduct, consideration should be given to whether the report may be considered a Public Interest Disclosure (PID) under the provisions of the [Public Interest Disclosures Act 2022](#). Reports of wrongdoing in a privacy related matter may relate to corrupt conduct or a government information contravention. Reports of wrongdoing made by public officials can attract the provisions of the [Public Interest Disclosures Act 2022](#) and should be referred to the PID co-ordinator or Chief Executive for consideration.



#### Further guidance:

- [Public Interest Disclosures \(PD2023\\_026\)](#)
- Section 4.3.4 Disciplinary matters and ICAC reporting

### 11.2.8 Law enforcement agencies, including police

#### HPP 11(1)(j)

HPP 11 allow health services to disclose personal health information to law enforcement agencies. In order to do so:

- the disclosure must be reasonably necessary to the functions of the law enforcement agency
- there must be reasonable grounds to believe that an offence may have been or may be committed.

#### 11.2.8.1 What is a 'law enforcement agency?'

The [Health Records and Information Privacy Act 2002](#) recognises the following agencies as law enforcement agencies:

- NSW Police or the police force of another State or a Territory
- Australian Federal Police
- NSW Director of Public Prosecutions (or equivalent office in another State, Territory or the Commonwealth)
- NSW Crime Commission

- Australian Crime Commission
- Corrective Services NSW
- Youth Justice NSW

#### 11.2.8.2 What sort of information can be provided?

The law enforcement exemption under HPPs 10 and 11 is very broad. It covers any health information relating to an offence which has or may be committed, provided that the information is 'reasonably necessary' to assist the law enforcement agency to perform its functions.

This exemption does **not oblige** health services to supply the information. Health services need to balance the important public interest in assisting law enforcement agencies to pursue their law enforcement and public protection functions with their own obligations of confidentiality to their patients and the sensitive nature of health information.

Generally, the information supplied should be limited to confirmation of identity and address.

The only exception is where the police can confirm they are actively investigating the commission of an offence and that the information is 'essential to the execution of their duty'. In such circumstances, there may sometimes be situations where additional, limited clinical information can be provided to the police, where appropriate. Careful consideration should be given to additional information provided, having regard to:

- The seriousness of the offence involved. For example, does it involve an offence involving serious physical harm, such as attempted murder or assault?
- The level of public risk. Is there an ongoing public risk or risk to particular individuals that would be addressed by the health service providing information (this also falls into HPP 11(1)(c), Disclosure to address a serious threat to health or welfare – see Section 11.2.3).
- The impact of the disclosure on patient care and the therapeutic relationship. The nature of the service being provided and the potential that the patient may discontinue obtaining care and treatment, should be considered, as well as the possible impact on the patient's mental state or wellbeing.

In some other circumstances, NSW Health policy may require reporting of a criminal offence or other conduct to the police or another agency. The NSW Health policy directive *Domestic Violence – Identifying and Responding (PD2006\_084)* states that in certain circumstances health staff must report to the police, regardless of the wishes of the victim. These circumstances may involve the victim

sustaining serious injuries such as broken bones; the perpetrator having access to a weapon and is making threats; or if there is an immediate risk to public safety or health staff are threatened.

After considering these matters, if a health practitioner decides it is appropriate to provide additional information, consultation should first occur with a more senior health care provider. Depending on the nature of the request, staff may also seek advice from the Privacy Contact Officer or a senior health service manager.

Other health information may only be provided with patient consent or in response to a search warrant or subpoena (see Section 11.3.6 Search warrants and subpoenas).



#### Further guidance:

- Section 11.3.4 Reporting 'serious criminal offences'
- Section 15.2 Requests from State and Federal Police

#### 11.2.8.3 Certificate of expert evidence

Evidence in court cases is generally provided verbally, through sworn evidence from each witness from the witness box, or via video link. Most witnesses to a court hearing will be lay witnesses. Lay witnesses (also known as a factual witness) will provide evidence of factual matters, on what they saw, heard or did.

Before a hearing, lay witnesses may voluntarily provide a written statement usually to a lawyer for the person who wants you to give evidence, outlining the facts known to that witness that is relevant to the court case. There is no obligation to provide a written statement. A lay witness is only allowed to provide relevant factual evidence. Witness statements are served on the parties to the court case, allowing each party the opportunity to prepare their cases. If a person provides a statement, they may be required to make themselves available to testify at the hearing. If a lay witness does not provide a statement, then that person may possibly be served with a subpoena ordering the person to attend Court. However, whilst this is possible it would be unusual. Lay witnesses are not to be allowed to provide their opinion on a matter.

An expert witness is a person who has specialised knowledge based on their training, study or experience. Unlike lay witnesses, an expert witness with specialist knowledge may express an opinion on matters within his or her area of expertise. Expert witnesses may provide information like a report, or a

statement detailing their opinion on a patient's medical record, or an opinion on a topic that is within their expertise. For example, an expert witness can assess a patient and provide a report on their assessment and provide an opinion, for example on the mental condition of a patient. Or an opinion on whether a patient's actions could have been involuntary at a particular time. Or a report on the properties of a particular drug and its likely effect on the patient. Unlike a lay witness statement, expert witnesses must include in an expert certificate that describes their knowledge based on his or her training, study or experience and an opinion that is based on their specialist knowledge based on his or her training, study or experience. The Evidence Act 1995 provides guidance on how the certificate should be drafted.

A request for a certificate of expert evidence is not a subpoena, search warrant or court order, and a health service is therefore not obliged to provide it nor does privacy law automatically 'authorise' release in this form. Therefore caution should be exercised prior to release, particularly where the doctor is no longer employed or is not otherwise available to review the patient's records on site prior to compiling the certificate. In circumstances where the health service decides to send patient records off-site to a doctor for review, these should be password protected (or de-identified, with the patient's identity provided to the doctor separately). Consideration of the public interest balanced with patient privacy should be made as described above (see Section 11.2.8.2 What sort of information can be provided?).

#### 11.2.8.4 How should requests from law enforcement agencies be handled?

Requests should be in writing on letterhead or via email, identifying the requesting officer, providing full address and contact details, and confirming the officer is a representative of a law enforcement agency. The request should also indicate the reason why the law enforcement agency is seeking the information.

Information should not generally be provided by telephone unless in response to a written request or where the requesting officer's identity can be verified.

Requests should be dealt with by the treating health care provider, a senior health professional or a health information manager. When information is provided the service provider should:

- limit access to information that is directly relevant to the inquiry and clearly necessary for the purpose

- document all instances of access in the health record (including any written requests from police)

#### Example

A paramedic attends a patient being held in a police holding cell. After the patient has been examined, the police officer asks questions about the patient relating to their health, and whether in the paramedic's opinion the patient is medically competent to be interviewed. The paramedic should only disclose information relating to the patient which is necessary to enable the police to monitor the condition of the patient, including symptoms which would require the patient to be taken to hospital. Paramedics are not required to discuss other matters relating to the patient, such as whether the patient is medically competent to be interviewed.

- where clinical information is necessary, this should be limited to a general outline of the patient's condition and/or injuries.

#### 11.2.8.5 Law enforcement requests in emergency circumstances

Where a health service receives a request for patient information which is urgently required to assist a law enforcement agency with an investigation, and it is impractical or unreasonable to receive this request in writing prior to disclosure, the senior treating clinician may provide limited patient information to the law enforcement agency verbally in person or via telephone.

Prior to release of information, the senior treating clinician must verify the caller's identity. This will require the requesting officer to provide their name, rank and command contact details (or equivalent). The senior treating clinician should then contact the command to confirm the caller's identity and be transferred to that officer.

The scope of the information provided to the law enforcement agency should be consistent with Section 11.2.8.2.

NSW Health has developed a protocol in partnership with NSW Police to assist staff with the sharing of personal health information following a serious motor vehicle accident. This protocol is titled '[NSW Police Force Crash Investigation Injury Assessment Protocol](#)'.

Other circumstances recognised by the [Health Records and Information Privacy Act 2002](#) which may involve an emergency response are:

### 1. 'Serious and imminent threat'

Disclosure of personal health information is permitted where the health service has reasonable grounds to believe this is necessary to lessen or prevent a serious and imminent threat to the life, health or safety of a person, or a serious threat to public health or public safety (see Section 11.2.3).

### 2. 'Finding a missing person'

Disclosure of personal health information is permitted to ascertain the whereabouts of a missing person reported to the police (see Section 11.2.6).

### 3. 'To assist in the stage of an emergency'

Use or disclosure of personal health information is permitted to assist in a 'stage of emergency' as defined in the [State Emergency and Rescue Management Act 1989](#) (fire, flood natural disaster, for example) (See Section 11.2.4).



#### Further guidance:

- Section 11.2.8.2 – What sort of information can be provided?
- Section 11.2.3 – To prevent a serious and imminent threat to health or welfare
- Section 11.2.6 – Finding a missing person
- Section 11.3.4 – Reporting 'serious criminal offences'
- Section 11.3.7 – Search warrants and subpoenas
- Section 15.2 – Requests from state and federal police

## 11.2.9 Investigative agencies

### HPP (10)(1)(j) & HPP (11)(1)(k)

The [Health Records and Information Privacy Act 2002](#) permits sharing of patient health information for the purpose of complaint handling or investigative functions by investigative agencies. A health service may use or disclose personal health information if this is **reasonably necessary** to the complaint handling or investigation functions of an investigative agency.

Under privacy law, an investigative agency is:

- the Ombudsman's Office
- the Independent Commission Against Corruption (ICAC) and the Inspector of ICAC
- the Law Enforcement Conduct Commission (LECC) and the Inspector of the LECC and any staff of the Inspector
- the Community Services Commission
- the Health Care Complaints Commission

- the Office of Legal Services Commissioner
- the Ageing and Disability Commissioner
- the NSW Office of the Children's Guardian
- any other person or body prescribed by Regulation for the purposes of the investigative agency definition.

In all cases where information is provided to an investigative agency, a health service must:

- as far as reasonably practicable, only respond to written requests which clearly set out the purpose for which the information is required and the provisions of the relevant Act under which the agency seeks the information
- seek and document proof that the person seeking the information is a representative of an appropriate investigative agency
- if in doubt about whether to supply the information, seek advice from the Health Information Service, Privacy Contact Officer or a senior manager
- provide access only to information that is relevant and necessary for the purpose
- document all instances of access in the health record
- where appropriate and practicable, inform the individual to whom the information relates of the access.

## 11.2.10 Disclosure on compassionate grounds

HPP 11(1)(g) and the [Health Records and Information Privacy Regulation 2022](#)

A health service may disclose relevant personal health information to an immediate family member for compassionate reasons. This only arises in relation to a 'disclosure' and will not apply to a use.

This exemption is intended to assist family members with understanding or coming to terms with events that have occurred to their close relative while in the care of the health service and understanding the circumstances of their death.

An immediate family member includes an individual person who is:

- a parent, child or sibling of the individual, or
- a spouse of the individual, or
- a member of the individual's household who is a relative of the individual, or
- a person nominated to an organisation by the individual as a person to whom health information relating to the individual may be disclosed.



The exemption is restricted as follows:

- the disclosure must be limited to 'what is reasonably necessary' for those reasons; and
- the individual must be deceased or incapable of giving consent; and
- the disclosure must not be contrary to any wish the individual has expressed and has not withdrawn, that the health service is aware of or could reasonably make itself aware of.

Before disclosing on compassionate grounds, consideration should be given to any health and safety concerns.

Disclosure is limited to a reasonable extent for those compassionate grounds; therefore, it is important to make a careful assessment of what part of the patient's health record is 'reasonably necessary' or 'relevant' to the family member making the request for access on compassionate grounds. As such, what will be reasonable will vary depending on the particular circumstances. For this reason, it may be appropriate to consult with treating clinical staff to identify the most appropriate types of information for disclosure.

For any requests for information on compassionate grounds, the health service should always ask the applicant if they are seeking information from multiple health services and districts as this can sometimes be more complex and requires special management as outlined in Section 11.2.10.2.

The purpose of the exemption is a compassionate one, and staff should consider that a 'compassionate' release of information may still be appropriate when family members are in dispute about access to information. Guidance can be sought from the Ministry of Health privacy team.

Disclosure on compassionate grounds would not generally cover release of an individual's entire health record and the amount of information disclosed will need to be considered on a case-by-case basis. An individual who seeks access to the entire health record should be advised to make a request for access under either the *Health Records and Information Privacy Act 2002* or the *Government Information (Public Access) Act 2009* (see Section 12 Patient access and amendment (HPPs 6, 7 & 8)), or otherwise to issue a subpoena via their legal representative. More guidance is provided below in 11.2.10.1.

Personal health information is covered by privacy principles until 30 years after a person has died. Relevant personal health information may be disclosed at any point in time under compassionate grounds. This may be relevant in circumstances where an immediate family member has been estranged and may want some information about a patient's death or illness some years after they have died.

If the immediate family member seeking access is under the age of eighteen, the health service must assess whether they have sufficient maturity to receive the information.

If information is being released on compassionate grounds in circumstances where a patient has died some time ago and a family member is requesting information after a significant lapse of time, there should be some evidence provided that the requesting party is an 'immediate family' member. This could be a birth certificate or marriage certificate linking the deceased with the requestor.

#### **11.2.10.1 Releasing information to families for legal claims after a patient has died**

Health services may receive requests from solicitors and family members to access records in situations where the release of the deceased's records is clearly for the purposes of litigation. In such cases, the most appropriate means by which a solicitor or family member may obtain health information about a deceased person is through a *GIPA Act* application or by court order, as the disclosure cannot be properly made on compassionate grounds. Further guidance can be sought from the GIPA Officer.

#### **11.2.10.2 Compassionate release involving multiple health services**

Some patients have complex and chronic health needs that are managed across multiple health services and Local Health Districts.

In the event of the patient's death (or incapacity), immediate family members may seek access to the patient's health care records on compassionate grounds to gain some closure or understanding.

It can be frustrating and confusing for family members when health services and districts have different processes for the disclosure of information on compassionate grounds. Sometimes this can be because the deceased or incapacitated relative gave strict instructions to one District about the management of their records but gave no



### Example

1. A young person is admitted to hospital unconscious and seriously ill, they have no identification, but their mobile telephone address book includes an entry for 'Mum at home'. You may contact the mother and inform her of her son's admission and general medical state.
2. A person has died suddenly at hospital without indicating his wishes to staff about how his personal health information should be dealt with. Two of the person's daughters, aged 15 and 17 arrive in a distressed state and wish to know the cause of death. In such case, the information could be shared with them, provided you have assessed they are sufficiently mature to cope.
3. A person with a history of drug use has died in hospital after a long AIDS-related illness. Before dying she has told hospital staff, she does not want her family to know the cause of death, as she had kept her drug use a secret. The family arrive and wish to know the cause of death. In such a case, you would be able to give only limited details.
4. A parent has died in hospital and one of their three adult children has been estranged from the family for some time. The other two children (who were on good terms with their parent) do not want their estranged sibling to have any information about their parent's death. The estranged child has contacted the hospital to find out what happened to their parent and the cause of death. Provided the parent did not express any wish to withhold information from the estranged child prior to their death, the hospital would be able to release limited details to the estranged child about their parent's illness and death, even if this was contrary to the wishes of the other two children.

restrictions on access to records in other Districts where they were treated.

Where matters like this arise and a patient had clinical care across multiple Districts, it is recommended that the Ministry of Health privacy team be consulted on coordinating responses to the family. This will assist in ensuring consistent approaches that accurately reflect the wishes of the deceased (or the patient who does not have capacity) and other relevant considerations.

This may also have relevance in cross-border communities where patients sometimes seek treatment across different states/territories for different health services.

#### 11.2.11 Chaplaincy services

Chaplaincy services are considered an important part of the health support services provided through

hospitals and other health services to patients and their families. Chaplaincy services are provided by trained accredited chaplains and trained accredited pastoral care workers (including volunteers) who are required to comply with privacy legislation. A regulation under the [Health Records and Information Privacy Act 2002](#) allows information to be provided to an accredited chaplain or pastoral care worker where this is a 'reasonable expectation' of the patient. The [Privacy Leaflet for Patients](#) informs patients that information about them may be provided to accredited chaplains and pastoral care workers.

Typically, a patient list is provided to accredited chaplains and pastoral care workers (including volunteers). This generally includes patient's name, religious affiliation (if this is provided to the health service) and ward location. Patient lists should only be released to accredited chaplains and pastoral care workers.

Further information about the patient's health care and treatment can also be disclosed to the accredited chaplain or pastoral care worker (including volunteers) involved in the patient's care where this is considered by the treating team to be relevant and appropriate.

With agreement from treating clinical staff, accredited chaplains and pastoral care workers may document significant pastoral and spiritual care intervention in the patient's health record. Further guidance is available in the [NSW Health & Civil Chaplaincies Advisory Committee NSW Memorandum of Understanding \(PD2011\\_004\)](#).

The patient may indicate at any time if they do not wish to receive chaplaincy services or if they do not want their information to be made available to accredited chaplains and pastoral care workers (including volunteers). The health service must ensure these wishes are complied with.



#### Further guidance:

- [NSW Health & Civil Chaplaincies Advisory Committee NSW Memorandum of Understanding \(PD2011\\_004\)](#)
- NSW Health [Privacy Leaflet for Patients](#)

## 11.3 Use and disclosure authorised by law – HPPs 10(2) and 11(2)

Privacy law recognises that there are many cases where a use or disclosure of information is either allowed by another law or is required by that law.

Where an agency seeks access pursuant to a lawful authorisation, the health service should:

- request written confirmation from the agency of the request and its legal basis
- provide only the information required by the authority
- check whether [\*Health Records and Medical/Clinical Reports – Charging Policy \(PD2006\\_050\)\*](#) applies to the request.

If there are doubts about the relevance of the documents to the purpose described in the law, staff should seek a written confirmation of relevance from the agency exercising their statutory power.

It is necessary to confirm not only that the requesting agency holds the legislative authority to require the information to be provided, but also that the circumstances set out under the relevant legislation apply to the case in question.

There are many such statutes, but some examples of those which commonly apply to a health service are set out below.

### 11.3.1 NSW Ministry of Health Officers and Environmental Health Officers

NSW Ministry of Health officers have powers under the [\*Health Services Act 1997\*](#) and the [\*Private Health Facilities Act 2007\*](#) to obtain information. Inspectors carry authorisations that indicate the nature of their powers and confirm their authority.

Section 42 of the [\*Poisons and Therapeutic Goods Act 1966\*](#), allows an officer of the NSW Ministry of Health to be appointed as an ‘inspector’ with powers to inspect and make copies of records relating to regulated goods, including records containing personal health information.

Environmental Health Officers from Public Health Units have powers under the [\*Public Health Act 2010\*](#) to obtain information. Inspectors carry authorisations that indicate the nature of their powers and confirm their authority.

### 11.3.2 Child protection

The information provided in this section is intended to provide a summary of the key issues relating to the balance between privacy and confidentiality and child protection. Details are provided in the following resources:

- [\*NSW Health Prevention and Response to Violence, Abuse and Neglect \(PARVAN\)\*](#)
- [\*Child Wellbeing and Child Protection Policies and Procedures for NSW Health \(PD2013\\_007\)\*](#)

- [\*Child Protection Counselling Services Policy and Procedures \(PD2019\\_014\)\*](#)
- [\*Child Wellbeing and Child Protection – NSW Interagency Guidelines for Practitioners\*](#)
- [\*NSW Interagency Mandatory Reporter Guide\*](#)

### Chapter 16A

Chapter 16A of the [\*Children and Young Persons \(Care and Protection\) Act 1998 \(Care Act\)\*](#) takes precedence over other laws regulating the disclosure of personal information, such as the [\*Privacy and Personal Information Protection Act 1998\*](#) and the [\*Health Records and Information Privacy Act 2002\*](#). Under Chapter 16A, each district is considered a separate prescribed body, rather than one single entity.

Chapter 16A provides for certain agencies, generally those working with children and families classed as ‘prescribed bodies’ under the [\*Children and Young Persons \(Care and Protection\) Act 1998\*](#), to exchange information with other prescribed bodies relating to a child’s or young person’s safety, welfare or wellbeing in certain circumstances.

Section 245B(3) of the [\*Children and Young Persons \(Care and Protection\) Act 1998\*](#) provides that Chapter 16A also applies to safety, welfare or wellbeing information relating to an unborn child who is the subject of a prenatal report (section 25) or a referral to a [\*NSW Health Child Wellbeing Unit\*](#) (section 27A). If a Health worker is unsure whether any report or referral has been made during the pregnancy, they can contact the NSW Health Child Wellbeing Unit for advice or, if after hours, the Child Protection Helpline.

Under Chapter 16A, information relating to the safety, welfare or wellbeing of a child or young person (including an unborn child who is the subject of a prenatal report) can be shared between prescribed bodies if the information is necessary to:

- inform any decision, assessment or plan or to initiate or conduct any investigation, or to provide any service, relating to the safety, welfare or wellbeing of the child or young person or class of children or young persons, or
- manage any risk to the child or young person (or class of children or young persons) that might arise in the recipient’s capacity as an employer.

A prescribed body for the purposes of Chapter 16A includes:

- the NSW Police Force
- a NSW government department or NSW public authority, including the Department of Communities and Justice (DCJ)

- a NSW government school or a NSW registered non-government school
- a NSW TAFE
- a NSW public health organisation or a NSW licensed private health facility
- a DCJ-accredited or DCJ-registered out-of-home care agency
- a DCJ-accredited adoption service
- the Family Court of Australia, the Federal Magistrate's Court of Australia, Centrelink and the Department of Immigration and Border Protection
- any other organisation which has direct responsibility for, or direct supervision of, the provision of health care, welfare, education, children's services, residential services, or law enforcement, wholly or partly to children
- nurses, medical practitioners, midwives, occupational therapists, psychologists and speech pathologists eligible for membership of Speech Pathology Australia.

Further information relating to Chapter 16A, including how to respond to requests and what to do if information is not to be provided, can be found in the relevant NSW Health policies.



#### Further guidance:

- [Child Wellbeing and Child Protection Policies and Procedures for NSW Health \(PD2013\\_007\)](#)
- [Responding to Sexual Assault \(adult and child\) Policy and Procedures \(PD2020\\_006\)](#)
- 12.5.3 Reports to the Department of Communities and Justice (DCJ)

## Section 248

Section 248 of the [Children and Young Persons \(Care and Protection\) Act 1998](#) allows for the exchange of information relating to the safety, welfare and wellbeing of a child or young person between DCJ and a prescribed body.

While generally DCJ will use Chapter 16A to request information relating to child protection, in some situations DCJ will require a prescribed body to provide information to them. If a section 248 request is made for personal health information to be provided, a NSW Health agency must comply with the direction. The information must be directly relevant to safety, welfare and well-being of a particular child or young person or class of children or young persons. Information can usually be provided by way of an extract from the health record. Full health records are not normally provided.



#### Further guidance:

- [Child Wellbeing and Child Protection Policies and Procedures for NSW Health \(PD2013\\_007\)](#)
- [Children and Young Persons \(Care and Protection\) Act 1998](#)

### 11.3.2.1 Reporting children and young people at risk of significant harm

**Under section 24** of the [Children and Young Persons \(Care and Protection\) Act 1998](#), a person who has reasonable grounds to suspect that a child or young person is at risk of significant harm may make a report to DCJ.

**Under section 27** of the [Children and Young Persons \(Care and Protection\) Act 1998](#) health staff must make child protection reports to DCJ where they have reasonable grounds to suspect that a child or young person is at risk of significant harm to DCJ, or to the NSW Health Child Wellbeing Unit Under section 27A.

**Under section 25** of the [Children and Young Persons \(Care and Protection\) Act 1998](#), health staff who have reasonable grounds to suspect, before the birth of a child, that the child may be at risk of significant harm when born may make a pre-natal report to DCJ.

Staff should use the online [NSW Interagency Mandatory Reporter Guide](#) to assist in determining whether a report to the Child Protection Helpline or to the NSW Health Child Wellbeing Unit is indicated.



#### Further guidance:

- [NSW Mandatory Reporter Guide](#)

### 11.3.2.2 Protection for mandatory reporters

Section 29 of the [Children and Young Persons \(Care and Protection\) Act 1998](#) provides for the protection of persons who make reports or provide certain information to DCJ or to the NSW Health [Child Wellbeing Unit](#).

Where access is being requested to reports made to DCJ, the identity of the staff member who made the report, or information from which the identity of that person could be deduced, is privileged and must not be disclosed, except with:

- the consent of the person who made the report,
- the leave of a court or other body before which proceedings relating to the report are conducted.

Where uncertainties exist regarding disclosure, or consideration is being made for the disclosure of the identity of a staff member who has provided

information to DCJ, advice should be sought from a health information manager, Privacy Contact Officer or legal officer at the health service or NSW Ministry of Health.

### 11.3.2.3 Protection for medical examinations

**Section 173:** Where a medical examination has been conducted in accordance with Section 173 of the *Children and Young Persons (Care and Protection) Act 1998*, a written report of the examination may be disclosed to the Department of Communities and Justice or the police.

Reports made under section 173 should be provided without charge by health staff. A health practitioner who transmits a report prepared under these circumstances is protected under the *Children and Young Persons (Care and Protection) Act 1998* from legal action in relation to allegations of professional misconduct and defamation.

### 11.3.2.4 Child Sexual Assault Medical Protocol: Sexual Assault Investigation Kit (SAIK)

The Child Sexual Assault Medical Protocol is the written protocol in the Sexual Assault Investigation Kit (SAIK). The SAIK includes consent to disclose SAIK records to DCJ and Police for medico-legal purposes. Chapter 16A of the *Children and Young Persons (Care and Protection) Act 1998* may still provide a basis of sharing this information outside the terms of the consent.

Special sensitivities arise in relation to SAIK records. Particular care should be given to each request for SAIK records to ensure that this information is not disclosed unless for a purpose permitted by the consent given at the time of the administration of the SAIK (or by another later consent) or where the request meets the requirements of Chapter 16A of the *Children and Young Persons (Care and Protection) Act 1998*. If it is not clear that the purpose for release is permitted by the consent, further details regarding the purpose of the request should be sought.



#### Further guidance:

- [Child Wellbeing and Child Protection Policies and Procedures for NSW Health \(PD2013\\_007\)](#)
- [Child Wellbeing and Child Protection – NSW Interagency Guidelines](#)
- [Photo and Video Imaging in Cases of Suspected Child Sexual Abuse, Physical Abuse and Neglect \(PD 2015\\_047\)](#)
- See section 11.3.2

- See Information sharing under section 248 of the *Children and Young Persons (Care and Protection) Act 1998*

### 11.3.2.5 Staff support

It is good practice for health staff to inform their supervisor or manager when they have received a disclosure from a child or young person, of reported abuse or neglect, to confirm an appropriate action plan or to inform their manager after they have taken relevant steps to respond to the child or young person. Child protection issues are complex and may raise both professional and personal issues for health staff. Informing a supervisor, Child Protection Coordinator or Child Protection Counselling Service, should issues arise, helps them to be aware that a staff member may need additional support, information or supervision. Health staff may also contact their Local Health District or Specialty Network for information about contacting the Local Health District Staff Counsellor or Employee Assistance Program (EAP).



#### Further guidance:

- [Child Wellbeing and Child Protection Policies and Procedures for NSW Health \(PD2013\\_007\)](#)
- [Child Wellbeing and Child Protection – NSW Interagency Guidelines](#)
- [NSW Interagency Mandatory Reporter Guide](#)
- [NSW Health Prevention and Response to Violence, Abuse and Neglect](#)

### Contact

- [NSW Health Kids and Families \(02\) 9391 9000](#)
- [NSW Health Child Wellbeing Unit 1300 480 420](#)

**For support and assistance in determining the level of risk of harm and how to respond to the needs of vulnerable children and young people.**

### 11.3.3 Disclosing health information of custodial patients

Sharing of custodial patient health information between Justice Health and Forensic Mental Health Network (Justice Health NSW) and Corrective Services NSW/Youth Justice NSW is detailed in *Justice Health NSW Guideline: 'Guidelines on use and disclosure of health information' (GL9.036)*. The Guidelines describe the circumstances where disclosure is authorised or required by the *Crimes (Administration of Sentences) Regulation 2014* (adults in custody) or the *Children (Detention Centres) Regulation 2015* (young people in custody). An example of a required disclosure under the *Crimes (Administration of Sentences) Regulation 2014* is found in clause 285, which provides that, where



a health officer forms an opinion that the mental or physical condition of an inmate constitutes a risk to the life of the inmate, or to the life, health or welfare of any other person, the health officer must report that he or she has formed that opinion and the grounds of the opinion to a Corrective Services NSW officer.

Justice Health NSW staff may disclose relevant information on the medical history or status of a custodial patient to Corrective Services NSW/Youth Justice NSW to investigate an incident or assault involving that patient where the law enforcement exemption applies (see Section 11.2.8). Requests should be in writing indicating the basis for disclosure. Consent from the patient must be obtained, unless other lawful disclosure applies (for example, risk of harm, see Section 11.2.3, or law enforcement, see Section 11.2.8).



#### Further guidance:

- [Justice Health NSW Guideline: 'Guidelines on use and disclosure of health information' \(GL9.036\)](#)

### 11.3.4 Reporting 'serious criminal offences' and 'child abuse offences'

Section 316 of the [Crimes Act 1900](#) requires a person to consider whether the information they have will be of 'material assistance' to securing the apprehension or conviction of a person for a 'serious criminal offence'. If it is, they are obliged to notify police. Failure to do so could lead to a conviction and the imposition of a penalty of up to five years imprisonment if there is no 'reasonable excuse' for this failure.

A 'serious criminal offence' is defined as an offence which attracts a penalty of five years imprisonment or more. Health staff should be aware that this covers offences such as drug trafficking, serious assaults, sexual assaults, murder and manslaughter. It does not cover minor drug possession offences or any offences under public health legislation.

The Regulations under the [Crimes Act 1900](#) also provide that prosecution for an offence under section 316 will not be commenced against a person without the approval of the Director of Public Prosecutions if the information was obtained in the course of practising as a:

- medical practitioner
- psychologist
- nurse
- legal practitioner

- social worker, including, a support worker for victims of crime, and a counsellor who treats persons for emotional or psychological conditions suffered by them.

The aim of the provision is to protect health care providers who, in good faith and on reasonable grounds, do not disclose this information to police.

Section 316 of the [Crimes Act 1900](#) also provides that there is a reasonable excuse for not reporting to police if:

- the information relates to a domestic violence offence or sexual offence against an alleged victim, and
- the alleged victim was an adult at the time the information was obtained by the person, and
- the person believes on reasonable grounds that the alleged victim does not wish the information to be reported to the police.

There is also a specific offence at s316A of the [Crimes Act 1900](#) relating to concealing child abuse offences.

Section 316A of the [Crimes Act 1900](#) requires a person to consider whether the information they have will be of 'material assistance' to securing the apprehension or conviction of a person for a 'child abuse offence'. If it is, they are obliged to notify police. Failure to do so could lead to a conviction and the imposition of a penalty of up to five years imprisonment if there is no 'reasonable excuse' for this failure.

The concealment of a child abuse offence includes concealment of a variety of sexual offences, serious assaults, and the failing of parental responsibility for a child. It has a maximum penalty of imprisonment for five years where the maximum penalty of the underlying child abuse offence is 5 years or more.

A person will not be guilty of the offence, however, if they have a reasonable excuse for not reporting the information to Police. This is similar to the existing requirement to inform Police of a serious indictable offence (section 316 of the [Crimes Act 1900](#)).

Reasonable excuses for not reporting information to Police include knowing or reasonably believing that:

- the information has already been reported under mandatory reporting obligations, such as to the Child Protection Helpline, NSW Health Child Wellbeing Unit or to the Ombudsman under the Reportable Conduct Scheme, or the person believes on reasonable grounds that another person has reported it
- the information is already known to Police
- the victim is an adult at the time of providing the



information and doesn't want it reported to the Police, or

- there are grounds to fear for their safety or another person's safety if they report to Police.



#### Further guidance:

- Section 11.2.8 Law enforcement agencies, including police
- [NSW Health Policy Directive Domestic Violence – Identifying and Responding \(PD2006\\_084\)](#)
- [Information sharing for service coordination, Department of Communities and Justice](#)

### 11.3.5 [Crimes \(Domestic and Personal Violence\) Act 2007](#)

Section 98M of the [Crimes \(Domestic and Personal Violence\) Act 2007](#) provides that an agency may, despite the privacy legislation, deal with information about a person without the consent of the person in certain circumstances.

Part 13A of the [Crimes \(Domestic and Personal Violence\) Act 2007](#) enables information to be shared without consent in some circumstances. It indicates that if consent is not provided by the person, or it is unreasonable or impractical to obtain consent, health services are permitted to share information under part 13A with [Safer Pathway Local Coordination Points](#) or other domestic violence support services, including NSW Police.

If disclosure is made under part 13A of the [Crimes \(Domestic and Personal Violence\) Act 2007](#), the risk must be serious, but there is no requirement of imminent risk.

Further guidance on information sharing under part 13A is set out in the [NSW Government's Domestic Violence Information Sharing Protocol](#). The Information Sharing Protocol's chapter on serious threat provides more detailed guidance to support service providers' decision making on sharing information without consent.

Section 13 of the [NSW Government's Domestic Violence Information Sharing Protocol](#) outlines details about sharing information where a serious threat is identified and provides guidance to support decision making where consent to share information is not provided. For further information about NSW Health's approach to managing disclosures under the [Crimes \(Domestic and Personal Violence\) Act 2007](#), see the NSW Health Policy Directive [Domestic Violence Routine Screening \(PD2023\\_009\)](#).

[NSW Health Information Bulletin, Use of Exchange of](#)

[Information Part 13A Crimes \(Domestic and Family Violence\) Act 2007 Form \(IB2016\\_056\)](#) provides assistance for NSW Health workers to comply with requirements under the [Crimes \(Domestic and Family Violence\) Act 2007](#).



#### Further guidance:

- [NSW Health Policy Directive Domestic Violence Routine Screening \(PD2023\\_009\)](#)
- [NSW Health Information Bulletin, Use of Exchange of Information Part 13A Crimes \(Domestic and Family Violence\) Act 2007 Form \(IB2016\\_056\)](#)
- [NSW Government's Domestic Violence Information Sharing Protocol](#)

### 11.3.6 Coroner

The [Coroners Act 2009](#) requires notification to the Coroner of deaths occurring under certain conditions. The Coroner will require a copy of the health records and sometimes may require the original records. In such cases, the health service should take care to ensure a full copy of all documents is retained by the health service. This is important in the event the death occurs outside of normal business hours and clinical staff are requested by police, on behalf of the Coroner, to provide the patient health records rather than the Health Information Department, which has strict protocols around disclosure.

Health records required for postmortem examinations must be provided to the Coroner in a timely manner to enable the pathologist or medical officer conducting the postmortem.

Where a request or an order is made by the Coroner or the police for coronial purposes and it is some time after the death, the Coroner should provide a Notice to Produce requesting the clinical records. The Notice should be received on letterhead (or electronic equivalent) with reference to section 53 of the [Coroners Act 2009](#), and detailing the information required.

A Coroner may request a copy of the final Serious Adverse Event Review (SAER) report. In that event, the District/SHN should provide the report so that the Coroner is aware of any recommended system changes that are relating to the incident. However, the final SAER report cannot, however, be tendered in evidence. If lawyers have been engaged to represent the District/SHN, the panel firm should forward the SAER report to the Coroner using a standard pro-forma letter which alerts the Coroner to sections 21O and 21P of the [Health Administration Act 1982](#). If lawyers are not engaged, the District/

SHN should provide a covering letter with the report noting that the SAER has been provided for information only and that pursuant to sections 21O and 21P of the [Health Administration Act 1982](#), it cannot be adduced or admitted in any proceedings.

For further information about the process involved with coronial requests, refer to the [Coroners Cases and the Coroners Act 2009 \(PD2010\\_054\)](#) and the [Incident Management Policy directive \(PD2020\\_047\)](#).



#### Further guidance:

- [Coroners Cases and the Coroners Act 2009 \(PD2010\\_054\)](#)
- [Incident Management Policy directive \(PD2020\\_047\)](#)

### 11.3.7 Search warrants and subpoenas

#### Search warrants

Compliance with a search warrant is required by law and record keepers should inform their immediate supervisor of any official demand for such access to information. Where possible, a copy of the record should be made and retained by the health service.

#### Subpoenas

Compliance with a subpoena is required by law. The return date should be noted on receipt and the subpoena dealt with promptly by the officer designated to co-ordinate responses to subpoenas.

Where a patient whose health record has been subpoenaed is not named as a party to the proceedings, they should be notified by the health service that the subpoena has been received and advised of the return date.

A subpoena may be challenged on a number of grounds including:

- abuse of process
- where the terms of a subpoena are excessively wide and imprecise, and to comply with them would be onerous
- public interest immunity
- legal professional privilege
- sexual assault communications privilege.

If a staff member has concerns about the scope of a subpoena, or considers it should be challenged, he or she should consult their immediate manager and obtain advice from the health service's solicitors, if appropriate.

Care should be taken that documents outside the scope of the subpoena are not provided by referring to the subpoena's schedule.

If acceptable, copies should be provided, and the original health record retained by the health service. Where originals are required, the health records should be forwarded to the Court and a complete copy kept by the health service.

Documents should be delivered to the Registrar or Clerk of the court in question by secure means, for example, courier delivery or registered post. A receipt signed by the official receiving the health record should be obtained which specifies the health record number, date received and name of the court. Some courts and tribunals accept subpoenaed material in an electronic format, such as on a USB device or via secure court portal. Where courts and tribunals (and other destinations external to NSW Health) do not have a secure portal, consideration should be given to sending any health information via eHealth's approved Secure File Transfer (SFT) service or other approved encryption services.



#### Further guidance:

- [eHealth NSW secure file transfer](#)
- [NSW Health Policy Directive, Subpoenas \(PD2019\\_001\)](#)

### 11.3.8 Health Care Complaints Commission

#### 11.3.8.1 Powers to enter premises

Authorised officers of the Health Care Complaints Commission (HCCC) have powers of entry that include the power to inspect, copy or remove health records and to require a person to provide information.

They carry authorisations that indicate the nature of their powers and confirm their authority. HCCC authorised officers can only exercise these powers with consent from the owner or occupier of the premises or with a search warrant.

#### 11.3.8.2 Powers to obtain documents

Under sections 21A and 34A of the [Health Care Complaints Act 1993](#), the Health Care Complaints Commission also has powers to require the production of documents, in order to assist it in the assessment of a complaint, or as part of its investigations. Where the Commission exercises this power, it should provide a written order for the documents, citing the relevant provisions.

### 11.3.9 The Ombudsman

The Ombudsman is empowered to require health authorities to supply information where a formal investigation is being conducted under the [Ombudsman Act 1974](#).

### 11.3.10 Official visitors

Official visitors are appointed under the NSW [Mental Health Act 2007](#) to inspect declared mental health facilities.

Under Section 132 of the [Mental Health Act 2007](#), official visitors must be provided with access to health records relevant to the care of patients.

### 11.3.11 Domestic Violence Death Review Team & Child Death Review Team

Chapter 9A of the [Coroners Act 2009](#) provides for a Domestic Violence Death Review Team, to review deaths occurring in the context of domestic violence in New South Wales. Section 101L requires public service agencies and health professionals to provide full and unrestricted access to records to the Team that it requires to fulfill its functions.

The Child Death Review Team is established under Part 5A of the [Community Services \(Complaints, Reviews and Monitoring\) Act 1993](#). The NSW Child Death Review Team and the Ombudsman review child deaths with the purpose of preventing and reducing child deaths. Under Section 34K of the [Community Services \(Complaints, Reviews and Monitoring\) Act 1993](#), the Child Death Review Team has powers to obtain unrestricted access to relevant health records and to obtain copies on request and it is the duty of public sector agencies to assist.

### 11.3.12 SafeWork NSW

Relevant sections of the [Work Health and Safety Act 2011](#) allow inspectors from SafeWork NSW (as the Regulator for the purposes of the Act) to require production of material relevant to the investigation of an alleged or possible breach of the Act. Such a request must usually be made either in writing stating the reasons why access is being sought, or a formal notice should be issued. Sections of the [Work Health and Safety Act 2011](#) relevant to the production or inspection of documents are:

- section 155 Powers of regulator to obtain information
- section 165 General Powers on entry (of an Inspector)
- section 171 Power to require production of documents and answers to questions
- section 174 Powers to copy and retain documents

### 11.3.13 NSW Ageing and Disability Commission

The purpose of the NSW Ageing and Disability Commission is to raise community awareness to reduce and prevent abuse, neglect and exploitation of older people and adults with disability. The

Commission receives and responds to reports or allegations of abuse, neglect and exploitation of an older person or adult with disability. Under the [Ageing and Disability Commissioner Act 2019](#), the Commissioner has the power to conduct an investigation and for the purpose of the investigation to issue notices to produce documents or other things, and to apply for a search warrant. A public health organisation and a government sector agency may also provide relevant information to the Commission in accordance with the Act.



#### Further guidance:

- [NSW Health Information Bulletin, 'Ageing and Disability Commissioner' \(IB2020\\_006\)](#)

### 11.3.14 Commonwealth Agencies

#### 11.3.14.1 Commonwealth Department of Social Services

The Commonwealth Department of Social Services has powers under the [Social Security \(Administration\) Act 1999 \(Cth\)](#) to access information relating to pensions, benefits and allowances. The request must be in writing and notice must be given under Sections 192, 196 and 197 of the Act.

#### 11.3.14.2 Veterans' Affairs

Under Section 128 of the [Veterans' Entitlements Act 1986 \(Cth\)](#), the health service is required to release to the Department of Veterans' Affairs (DVA) relevant information relating to treatment received at any public health facility by repatriation beneficiaries.

Deaths of repatriation patients must also be reported to the DVA.

Disclosure of the names of DVA patients for the purpose of visits by voluntary groups, such as ex-service organisations, is only permitted with patient consent. Pro forma consent forms and information leaflets are available from the health service's DVA representative, or by contacting the [Government Relations Branch, Ministry of Health](#).

#### 11.3.14.3 Immigration and border protection – Illegal Non-Citizens

The Commonwealth Department of Home Affairs has powers under section 18 of the [Migration Act 1958 \(Cth\)](#) to obtain information about illegal non-citizens.

The power allows the Department of Home Affairs to require a health service to produce information believed to be relevant to ascertaining the identity or whereabouts of a person believed to be an illegal non-citizen. The power must be exercised by service of a notice in writing.

### 11.3.15 Statutory reporting requirements

The public health system is required to notify authorised agencies of certain types of personal health information. The following must be reported to the Ministry of Health:

- scheduled Medical Conditions and Notifiable Diseases
- inpatient statistics
- maternal and perinatal data for Perinatal Data Collection
- cancer cases (through the NSW Cancer Registry)
- congenital conditions (Register for Congenital Conditions).



#### Further guidance:

- Section 15.9.6 Managing public health risks
- [NSW Health Admission Policy \(PD2017\\_015\)](#)
- [Notifying Cancer-Related Data to the NSW Cancer Registry \(PD2022\\_008\)](#)
- [NSW Register of Congenital Conditions – Reporting Requirements \(PD2018\\_006\)](#)
- [Notification of Infectious Diseases under the NSW Public Health Act \(IB2013\\_010\)](#)
- [Notifiable Conditions Data Security and Confidentiality \(PD2012\\_047\)](#)
- [Notification of Acute Rheumatic Fever and Rheumatic Heart Disease – the NSW Public Health Act 2010 \(IB2015\\_057\)](#)

#### Health Services Act 1997

Chief Executives of health services have an obligation to report suspected unsatisfactory conduct or suspected professional misconduct of staff members or contracted service providers (VMOs) to the relevant health professional Council.

#### Adverse drug reactions

Adverse drug reactions must be reported in accordance with the [Medication Handling Policy \(PD 2002\\_032\)](#).

#### Home and Community Care Act 1985 (Cth)

The Commonwealth Home and Community Care (HACC) Program provides services that support older people to stay at home and be more independent in the community. The [Home and Community Care Act 1985 \(Cth\)](#) requires HACC service providers, which may include some NSW Health agencies, to operate within the reporting framework set out in their Aged Care Funding Agreement. This agreement requires the reporting of demographic and health details relating to individuals receiving HACC services.



#### Further guidance:

- [Home and Community Care Minimum Data Set Version 2 – Collection & Reporting Requirements \(PD2008\\_050\)](#)

#### Poisons and Therapeutic Goods Act 1966

The NSW Ministry of Health collects and maintains personal health information as required under the [Poisons and Therapeutic Goods Act 1966](#).

The [Poisons and Therapeutic Goods Act 1966](#) provides for the collection, use and disclosure of personal health information as follows:

- for the purpose of administering authorisations to prescribe drugs of addiction
- to the Medical Committee and its subcommittees for the purpose of advising on applications to prescribe drugs of addiction
- under the provisions of Section 43 of the Act when auditing and investigating individual health practitioners and licensed or authorised persons or organisations to ascertain compliance with the Act or Regulation.



#### Further guidance:

- [NSW Health Pharmaceutical Services Unit](#)

### 11.3.16 Information required by the Minister or Premier

NSW privacy laws also recognise that from time to time the executive arm of government (for example, the Minister for Health and the Premier) may require access to and use of personal health information.

HPPs 10(4) and 11(4) therefore provide that nothing in the use and disclosure restrictions prevents the disclosure of personal health information by a public sector agency:

- to another public sector agency under the administration of the same Minister if the disclosure is for the purposes of informing that Minister about any matter within that administration; or
- to any public sector agency under the administration of the Premier, if the disclosure is for the purposes of informing the Premier about any matter.

#### 11.3.16.1 Ministerial correspondence and briefings

NSW Health agencies are required to prepare correspondence and briefings for, and on behalf of, the Minister for Health, Minister for Mental Health and the NSW Premier as requested. Such requests may seek to include personal health information about the correspondent, or a person they claim to represent.



When responding to correspondence, staff should take care not to disclose personal health information other than that which has been provided by the correspondent, or with the consent of the patient, or as is necessary to appropriately address the concerns raised and provide relevant background information to the Minister.

Care should also be taken when responses are being prepared in consultation with more than one health service or district, to ensure that only relevant health information is accessible for the purpose of the response.

If the correspondent is seeking to obtain access to or a copy of their own health record, or that of a friend or relative, they should be referred to the Health Information Service, or equivalent, for the health service where the patient received health services (see also Section 12 Patient access and amendment).



#### Further guidance:

- Section 11.2.2.1 Where a third party seeks access

## 11.4 Computer systems and applications

Staff with access to NSW Health electronic applications, such as an electronic health record and the My Health Record, may only access, view and use or disclose information held in the system for purposes directly related to their work.

This means NSW Health staff may only view, access, use and disclose personal health information when it is necessary for them to do so to carry out their work duties, whether that be patient care or other work duties that require access to personal and health information like patient billing or human resource management.

If in doubt about their obligations, staff should seek advice from a senior manager, local Health Information Manager or Privacy Contact Officer.

Staff should be provided with the appropriate level of access to physical and electronic health records (for example, full, partial or no access) in accordance with their role and their work requirements. In compliance with NSW Health policies on information security, a secure physical and electronic environment must be maintained.

NSW Health electronic record systems are auditable

so staff access can be reviewed following privacy complaints or because of systematic auditing.



#### Further guidance:

- Section 9 Retention, Security and Protection
- Section 16 Electronic Health Information Management Systems

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

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

The *Health Records and Information Privacy Act 2002* allows a person to apply for access to information a health service holds about them.

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

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

Health services should have governance systems in place to manage patient requests for access to their health information, including data held on remote patient monitoring platforms (RPMP). Remote



monitoring uses technology to collect and send a patient's medical and healthcare data to an app, device or service.



#### Further guidance:

- [How do I use virtual care?](#)

## 12.2 Interaction of HRIP Act and the GIPA Act

The general principle under both privacy laws and the *Government Information (Public Access) Act 2009* (GIPA Act) is that **a person will be presumed to have a right to access the information an organisation holds about them.**

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

### 1. Mandatory Disclosure

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

### 2. Informal Release

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

### 3. Proactive Release

Agencies are encouraged to release as much information as possible, free of charge or at the lowest reasonable cost.

### 4. Formal Access

If information cannot be accessed as above, a formal access application may be necessary.

As a general principle, health services should rely on the access provisions in privacy law rather than the GIPA Act and integrate its principles into their day-to-day work. In practice, NSW Health agencies generally process applications for health information under the *Health Records and Information Privacy Act 2002* as this is a less onerous process for both the agency and the applicant.

The GIPA Act should however still be used where:

- The patient (or their legal representative) declines access under the *Health Records and Information Privacy Act 2002* and specifically requests access

under the GIPA Act. Their application should be processed under the GIPA Act and should not be refused simply because they choose not to use the *Health Records and Information Privacy Act 2002*.

- The information sought relates to a number of people (or 'third parties') or is sought in the context of a family dispute or raises other contentious issues. The GIPA Act provides a structured process for consultation with people other than the applicant who may be affected by release of information. It will therefore be a useful alternative in such cases.
- A family member seeks information about a relative who is deceased, and there is no appropriate 'authorised representative' to consent to the disclosure.
- The information sought is not limited to the personal health information of the applicant, but includes other government information such as incident reports that may require consultation and assessment of public interest considerations for or against release.

Even if the application is under the *Health Records and Information Privacy Act 2002*, agencies need to be mindful of matters that may need consideration under the provisions of the *Government Information (Public Access) Act 2009*, if for example consultation with a third party needs to occur or where there are public interest considerations against disclosure.



#### Further guidance:

- Section 12.3.1 Reasons for refusing access under the GIPA Act
- Refer to local Health Information Service for advice on local processes for access under the *Health Records and Information Privacy Act 2002* and the *Government Information (Public Access) Act 2009*
- Section 4.2.2 *Government Information (Public Access) Act 2009*
- Section 15.10 Deceased persons

## 12.3 Where access is refused

The *Health Records and Information Privacy Act 2002* recognises that sometimes circumstances will arise where access may be refused. This is most often likely to arise where access may place the person seeking their information, or another person, at risk of harm. **HPP 7** therefore allows refusal of access if a refusal 'is authorised or allowed under a law'.

This provision is designed to recognise circumstances where access could be refused under the *Government*

Information (Public Access) Act 2009 or any other law. For example, if access can be refused on this basis under the Government Information (Public Access) Act 2009, the health service will be ‘lawfully authorised’ to refuse access under the Health Records and Information Privacy Act 2002. However, in such circumstances, decision making should be clearly documented, including in which circumstances access will not be granted, which considerations were made to determine whether to disclose or not disclose certain information, and the professional status of the person who has made that decision.

There may also be other grounds for refusal in the Government Information (Public Access) Act 2009. Staff should refer any enquiries to their local GIPA Right to Information Co-ordinator.

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

### 12.3.1 Reasons for refusing access under the GIPA Act

The Health Records and Information Privacy Act 2002 access provisions focus on individuals accessing their own medical and health information. As such, it will be rare to refuse access.

Whilst a person is presumed to have the right to access information about them (or the person they represent), the Government Information (Public Access) Act 2009 requires an agency to consider whether it is in the public interest to disclose the information.

The most common circumstances where access may be refused for public interest reasons under the Government Information (Public Access) Act 2009, and therefore also under the Health Records and Information Privacy Act 2002, are set out in the Government Information (Public Access) Act 2009 (see section 14, Table clause 3), and are provided below.

#### 12.3.1.1. The disclosure of information could reasonably be expected to reveal another individual’s personal information

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

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

- where this information is already known to the patient

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

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

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

- whether disclosure of the third-party information could endanger the life or physical safety of any person
- whether disclosure of the third-party information may reveal the personal health information of any person (including details such as Hepatitis C or HIV status)
- whether disclosure of the third-party information relates to views, events or circumstances which the patient, or the person seeking access, may not be aware of, and it would be unreasonable in the circumstances to disclose this information.



#### Further guidance:

- Refer to local Health Information Service for advice on local processes for access under the Health Records and Information Privacy Act 2002 and Government Information (Public Access) Act 2009
- See Section 4.2.2 Government Information (Public Access) Act 2009.

#### Carer details

Health records may contain details about the patient’s carer, particularly records relating to children and young people in out-of-home care, people with a disability and older people. Care must be taken not to disclose carer details where it is not evident that this information is already known to the patient, or person acting on behalf of the patient. See Section 11.3.2.6. Children and young people in out-of-home care (OOHC).

#### Staff details

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

- disclosure could reasonably be expected to expose the staff member to a risk of harm
- other privileges apply, such as in the case of a report to Department of Communities and Justice, where all references to the staff ‘reporter’ are to be removed, including previous or subsequent entries made in the health record of their name or

designation. Other notations of a report being made should also be removed.

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

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

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

In rare circumstances where the treating health practitioner considers access could be prejudicial to the physical or mental health of the patient or to another person, the health record may be referred to a third party such as an independent health practitioner for assessment. If this occurs, the health record plus the assessment should then be referred to the Department Head or Director of Medical Services for review and a decision made as to whether the applicant should be granted access to all or part of the health record. In some cases, it may be necessary for access to be provided via a health practitioner nominated by the applicant (See below and s73(3) [Government Information \(Public Access\) Act 2009](#)).

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

#### **Example**

A patient of a sexual health service has a referral letter on their file from a previous service provider. The referring clinic has detailed the HIV status of the patient's former partner in the correspondence. The HIV status of the former partner is third party information. This means that care must be taken not to release the former partner's HIV status, unless there is a legal requirement to do so, or consent has been obtained from the former partner. In circumstances where the third party does not consent to the release of their HIV status or other sexual history, all references to the third-party information must be blacked out (redacted) prior to any access being provided to the health record.

#### **Example**

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

Where it is determined that access will not be granted under the [Health Records and Information Privacy Act 2002](#), then reference should be made to section 14 of the [Government Information \(Public Access\) Act 2009](#) (see Section 12.4 Providing access). Consideration should then be given to the public interest considerations against disclosure and whether conditions should be placed on the release of the health information.

### **12.3.1.3 Disclosure of personal information about a child would not be in the best interests of the child**

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

### **12.3.1.4 The disclosure of information could reasonably be expected to contravene an IPP or HPP**

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

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

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

## 12.4 Providing access

### Example

The child's parents are separated. The child lives with her mother but sees her father on alternate weekends. There are no parenting orders in place and each parent is entitled to seek access to the child's health record. The child's relationship with her father has been strained but is improving and to this end she has been seeing a community social worker. Her father has sought access to these counselling records and the clinicians are concerned that the child's progress (and her relationship with her father) will deteriorate if he has access to these health records. The clinicians may rely upon the public interest considerations against disclosure in the *Government Information (Public Access) Act 2009*, section 14, to refuse the father's access to these health records, namely, that the disclosure of personal information about the child would not be in the best interests of the child (see the *Government Information (Public Access) Act 2009*, Section 14, Table clause 3(g)). The clinicians will also need to provide the father with a reason for this decision, as it is not sufficient to only quote the legislation. Guidance can be sought from Ministry of Health, Legal and Regulatory Services Branch.

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

- electronic or paper copy (where the information is emailed outside of NSW Health, it must be transmitted securely for example, using NSW Health approved secure file transfer software, or another method to secure the information e.g. by use of a password or encryption).
- direct access, by supervised viewing of the health record on the health service's premises. A health practitioner or health information manager must always supervise access to health records. Patients may request the assistance of a health practitioner in interpreting the health record
- a copy sent to a health practitioner nominated by the applicant as allowed for in the *Government Information (Public Access) Act 2009*, Section 73(3), which states:  
*'A condition may be imposed that access to medical*

*or psychiatric information will only be provided to a health practitioner nominated by the applicant and not to the applicant personally.'*

It is at the discretion of the health service to determine whether this is necessary, for example:

- where the applicant might be assisted by an in-person review of the records to prevent misinterpretation
- where there is a *risk of harm* to the applicant or any other person or child, which could be avoided if access is provided via a health practitioner
- where the applicant has requested access via a health practitioner
- copies sent to a third party, such as an insurance company, solicitor, or legal representative. This should only occur where the third party clearly acts for the applicant or has made the application on his or her behalf and has provided written consent from the patient.

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

The requirements for application for access to records by patients mirror the requirements for third-party access. See Section 11.2.2.1 Where a third party seeks access.

Copies of health records may also be provided to family members on compassionate grounds. See Section 11.2.10 Disclosure on compassionate grounds.



### Further guidance:

- See email security advice in chapter 1-10 of the Manual.

## 12.5 Other conditions of access

### 12.5.1 Parenting orders

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

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

One parent's request for the other parent not to access the child's health record cannot of itself be a basis to refuse access, unless there are reasonable grounds to believe that this access would put the



child, or another person, at risk of harm. Consultation with 'Violence, Abuse and Neglect' Managers or the [NSW Health Child Wellbeing Unit](#) should occur in these circumstances.



#### Further guidance:

- Section 11.3.2. Child protection
- Section 12.3.1.3 The disclosure of personal information about a child would not be in the best interests of the child

### 12.5.2 Apprehended Violence Order

Where there is an Apprehended Violence Order (AVO)\* against a parent, this does not affect their right to **apply** for access to health information relating to their child. As with all applications, care should be taken not to disclose personal details, such as address details, personal or health information about a third party which may be included in the child's health records. Consultation with 'Violence, Abuse and Neglect' Managers or the [NSW Health Child Wellbeing Unit](#) should occur in these circumstances.

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

### 12.5.3 Reports to the Department of Communities and Justice (DCJ)

Section 29 of the [Children and Young Persons \(Care and Protection\) Act 1998](#) provides for the protection of persons who make reports or provide certain information to Department of Communities and Justice (DCJ).

Where access is being requested to reports made to DCJ, the identity of the staff member who made the report, or information from which the identity of that person could be deduced, is privileged and must not be disclosed, except with:

- the consent of the person who made the report
- the leave of a court or other body before which proceedings relating to the report are conducted.

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



#### Further guidance:

- Section 11.3.2 Child protection

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

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

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

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

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

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

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

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



#### Further guidance:

- Section 11.2.1 Directly related purpose



- Section 11.2.2 Consent
- Section 15.6 Legal claims and insurance
- Section 9.2.4 Secure File Transfer (SFT) and other systems

## 12.6 Obtain proof of identity

When seeking access to personal health information, applicants must provide proof of identity in a form approved by the health service.

This may include a certified copy of any one of the following documents:

- current Australian driver's licence
- current Australian passport
- other proof of signature and current address details (2 proofs of identity may be required in this case)
- approved translations of foreign documents, where relevant.

Ideally, any proof of identity should include a photo identification. A certified copy requires the signature and authorisation by a Justice of the Peace (JP) or solicitor to certify that it is a true copy of the original document. Identification does not have to be certified if the identity can be verified in other ways, including cross-checked against other documents held in the medical record, for example.

Sometimes patients will present in person and staff will sight original documents or electronic versions (via the Service NSW or Medicare Apps).

If applying by mail, certified photocopies of identification can be accepted. If applying by email, a scanned version of the certified copies of identification documents can also be accepted.

Where appropriate and available, electronic verification of identity tools may also be acceptable for proof of identity. In addition to the above minimum requirements, a health service may also require further proof of identity at their discretion.

Depending on the circumstances and the types of information being released, different ID requirements may be appropriate.

Whatever method is used, it is important that the health service takes reasonable security safeguards in terms of the management, security and access to this information.

[State Records NSW](#) have provided recommendations on the approach when assessing identity documents

such as driver's licences, passports, Medicare cards, or Council rate statements:

*Many public offices need to sight proof of identity or other documents as part of an application process. These are transitory documents that in most cases need to be sighted but not retained. We recommend:*

- *proof of identity documents should be returned without copying them and public offices should capture a record that the identity documents have been sighted*
- *where a copy is required for verification purposes or transmission to another public office, dispose of the copies as soon as business use ceases.*

This same principle applies to credit card details and medical certificates – if there is no need to retain the originals or copies of the originals once the transaction is completed, they can be returned or securely disposed of.

Creating a record that the documents were sighted fulfills the requirements of the *State Records Act 1998* and the retention and disposal authorities.



### Further guidance:

- [NSW Health Electronic Information Security Policy Directive \(PD2020\\_046\)](#)
- [Communications – Use & Management of Misuse of NSW Health Communications Systems \(PD2009\\_076\)](#)
- [State Records NSW](#)
- Section 9.2.4 [Secure File Transfer \(SFT\)](#) and other systems

## 12.7 Fees and charges

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

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



### Further guidance:

- [Health Records and Medical/Clinical Reports – Charging Policy \(PD2006\\_050\)](#)
- [Health Records and Medical/Clinical Reports – Rates \(IB2019\\_036\)](#)

## 12.8 Additions, corrections and addendums (HPP 8)

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

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

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

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

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

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

### 12.8.1 Where an alteration is included

Untraceable alterations or deletions to clinical information held in the health record should not be made. Original incorrect entries should not be erased but lined through, or otherwise appropriately amended to reflect the correct information, so the original entry remains retrievable and readable. This requirement applies where the entry relates to clinical care or medical opinion. Standard updates to demographic and other similar details, general practitioner contacts etc., will not need to be lined through but simply updated.

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

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

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

### 12.8.2 Where an alteration is refused

If the changes requested by the patient (or other authorised party) do not meet the requirements of accuracy, completeness, etc. as set out in HPP 8(1), the health service is required in HPP 8(2) to take

such steps as are reasonable to attach additional information as an addendum to the health record. In addition, the patient's own comments should be attached as an addendum to the health record on request, along with an explanation of the circumstances.

# 13 Miscellaneous (HPPs 12, 14 & 15)

## 13.1 Identifiers (HPP 12)

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

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

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

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

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

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

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



**Further guidance:**

- [Healthcare Identifiers Act 2010 \(Cth\)](#)

## 13.2 Transferring personal health information out of NSW (HPP14)

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

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

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

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

### 13.2.1 Within Australia

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

- the private sector is covered by the [Privacy Act 1988 \(Cth\)](#)
- all states and territories in Australia either have equivalent privacy laws or binding public sector policies across their respective systems.

This ensures that HPP 14 does not limit the ability for health services to share information in Australia (noting HPP 11 must still be complied with).

### 13.2.2 Outside Australia

Sharing of information with health services outside Australia needs to be considered on a case-by-case basis. Even where a country has privacy laws, the receiving entity may not be bound by those laws.

In relation to other external jurisdictions, health services should:

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

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

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



#### **Further guidance:**

- Seek advice from Ministry of Health Legal and Regulatory Services.

## 13.3 Linkage of health records (HPP 15)

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

HPP 15 will apply to the linkage of health records at a state or national level between the public and private sectors, or between two or more private health services. HPP 15 will apply if the systems being linked are ongoing records of health care. It requires that such a linkage system must be 'opt-in', i.e. that a patient must give 'express consent' to the inclusion of their health information in the health records linkage system.

There are two exemptions to HPP 15. These are:

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

The My Health Record is exempt from the requirements of the HPP 15 as are some NSW Health records linkage systems used by some private providers that are required for the normal operation of health services.



#### **Further guidance:**

- Express consent at Section 5.4.3



# 14 Complaints handling and responding to breaches

This chapter summarises considerations when handling privacy complaints and data breaches affecting health information. Breaches may be identified as a result of a consumer's privacy complaint or may also be identified by the health service before consumers are aware that their health information has been affected by a breach. This chapter summarises how to respond to consumer complaints and to breaches that are identified by the health service.

All privacy complaints, reports of privacy or data breaches, and requests for privacy internal review should be treated as serious matters and must be referred to the Privacy Contact Officer.

## 14.1 General complaint handling principles

People who have a privacy complaint against a health service should be informed of their right to make a formal application for a privacy internal review. Complainants should also be given the option to have the complaint addressed quickly and informally as an alternative to privacy internal review.

A formal complaint would generally include:

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

The [Health Records and Information Privacy Act 2002](#) requires health services to use the internal review process set out in Part 5 of the [Privacy and Personal Information Protection Act 1998](#). Guidelines for management of complaints using these processes are set out in [NSW Health Privacy Internal Review Guidelines \(GL2019\\_015\)](#). If health services receive a complaint under privacy legislation, this Guideline must be referred to and the local privacy contact officer notified of the complaint.

Staff must also notify complaints in the NSW Health incident management system and follow the procedures outlined in the [Incident Management Policy Directive \(PD2020\\_047\)](#).

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

## 14.2 Privacy internal reviews

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

The focus of an internal review is the conduct of the agency concerned:

*A person (**the applicant**) who is aggrieved by the conduct of a **public sector agency** is entitled to a review of that conduct.*

On receipt of a Privacy Internal Review application, guidance can be sought from the Ministry of Health privacy team and the [NSW Health Privacy Internal Review Guidelines \(GL2019\\_015\)](#)

Any privacy complaint must be in writing, addressed to the health service concerned and made within six months of the individual becoming aware of the alleged contravention (unless the health service agrees to a longer timeframe). See Section 4.4 of the [NSW Health Privacy Internal Review Guidelines \(GL2019\\_015\)](#) for further guidance.

A person is not required to identify the particular HPP which is the subject of the complaint. Health services are obliged to review any such complaint received and to identify the specific HPPs which may have been breached. The internal review provisions allow individuals to seek a review of certain conduct of an agency, in circumstances where the individual believes that the agency has breached the terms of the privacy laws.

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

Where the person's concerns cannot be resolved through referring to existing policies and guidelines, an agency must provide the person with information relating to their rights to an internal review under privacy law, and the requirements for lodging a valid application.

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

An individual may also complain on behalf of someone else if they are authorised to act on their behalf (for example, with the applicant's consent or if they are a parent or guardian), or an individual may complain if they are aggrieved by the handling of someone else's personal or health information and such a complaint may also require a privacy internal review.



#### Further guidance:

- [NSW Health Privacy Internal Review Guidelines \(GL2019\\_015\)](#), see Section 4
- [IPC Fact Sheet – making a complaint about a NSW public sector agency](#)

## 14.3 NSW Civil and Administrative Tribunal (NCAT)

If the complainant is not satisfied with the outcome of the internal review, the complainant may appeal to the [NSW Civil and Administrative Tribunal \(NCAT\)](#).

Where a complainant lodges an application to NCAT, the health service should notify:

- the NSW Ministry of Health Legal Unit at: [moh-significantlegalmatters@health.nsw.gov.au](mailto:moh-significantlegalmatters@health.nsw.gov.au)
- Privacy Contact Officer, Ministry of Health, at: [moh-privacy@health.nsw.gov.au](mailto:moh-privacy@health.nsw.gov.au)
- the Treasury Managed Fund (TMF).

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

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



#### Further guidance:

- [NSW Health Privacy Internal Review Guidelines \(GL2019\\_015\)](#)

## 14.4 Responding to data breaches

A data breach involving personal health information occurs when there is an unauthorised access, disclosure or loss of that information. A data breach does not need to be caused by a deliberate or willful act. When a data breach occurs, the organisation no longer controls the personal health information for which it is responsible.

NSW Health organisations must implement the minimum standards outlined in the [Data Breaches involving Personal or Health Information \(PD2023\\_040\)](#) when responding to data breaches affecting personal health information or personal information.

The NSW Mandatory Notification of Data Breach (MNDB) scheme applies to data breaches affecting personal health information or personal information which involve a risk of serious harm. The scheme mandates notification of eligible data breaches to the NSW Privacy Commissioner and affected individuals.



#### Further guidance:

- [Data Breaches involving Personal or Health Information \(PD2023\\_040\)](#)

## 14.5 Breach of privacy by an employee

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

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

An internal review will determine whether such a privacy breach was attributable to the operation of the health service. Privacy breaches caused by employees when they are acting in their personal capacity rather than in their work or professional role may not be attributable to the health service if it has exercised all reasonable care to prevent breaches through measures such as privacy training, education and appropriate information security safeguards. However, the matter may warrant a misconduct investigation into the employee's conduct.

Referral of staff to Workforce must be considered in any incident of unauthorised staff access to health information. Where it is found, or suspected, that a staff member has used or disclosed health information without authorisation the health service should investigate the allegations in accordance with the NSW Health Policy directive, [Managing Misconduct \(PD2018\\_031\)](#).

When a breach of privacy by an employee is confirmed, action taken by the health service should be commensurate with the nature, scale and seriousness of the breach. Action can range from counselling or training to formal disciplinary action (warning, termination). Any actions must comply with relevant NSW Health policies.



#### Further guidance:

- [Managing Misconduct \(PD2018\\_031\)](#)
- [Managing Complaints or Concerns about Clinicians \(PD2018\\_032\)](#)
- [Public Interest Disclosures \(PD2023\\_026\)](#)
- [NSW Health Privacy Internal Review Guidelines \(GL2019\\_015\)](#)

# 15 Common privacy issues

Sometimes staff require further information about privacy issues arising in their broader interactions with other agencies, specific projects or matters that cut across the HPPs. In recognition of this, Section 15 provides a guide to some common privacy issues in NSW Health.

## 15.1 Third party health care providers

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

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

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

### 15.1.1 Informing patients

Patients should be made generally aware that:

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

The NSW Health [Privacy Leaflet for Patients](#) includes this information.



#### Further guidance:

- Section 7 Collecting personal health information (HPPs 1-4)
- [Privacy Leaflet for Patients](#)

### 15.1.2 Health practitioner obligations

Recognition that health care providers involved in ongoing care may access patient information ensures service providers have ready access to information relevant to care. Health care providers also have both a legal and professional obligation to ensure they exercise this right appropriately.

### 15.1.3 Addressing patient concerns

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



#### Further guidance:

- Section 15.9 Information-specific laws and policies
- [Your Health Rights and Responsibilities](#)
- [Sexual Safety of Mental Health Consumers Guidelines](#)

### 15.1.4 Conclusion of care

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

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

### 15.1.5 Discharge referrals to GPs and others

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

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

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

### 15.1.6 Records of a patient's family members

Requests by health care providers for access to the health records of their patient's family members must be managed like any third party, genetic or compassionate access request or be accompanied by the written consent of the person to whom the health record relates (or an authorised representative).



#### Further guidance:

- Section 5.6 Authorised representative
- Section 11.2.3.5 Genetic information
- Section 15.9.3.3 Third party access – genetic relatives
- Section 11.2.10 Disclosure on compassionate grounds
- Section 12 Patient access and amendment (HPPs 6, 7 & 8)

## 15.2 Requests from state and federal police

### 15.2.1 Where disclosure to police is authorised by patient

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

Where a patient has authorised the police to have access to information from the patient's health records, the records can be provided to the police following receipt of a written request by the police and a documented patient consent. The health information should be assessed, and the disclosure limited to fit the terms of the request and consent. Clinical staff should liaise with the Health Information Service, or facility equivalent, prior to release of information to police.

For considerations concerning records relating to domestic or family violence, child protection or sexual assault, contact PARVAN [\*Prevention and Response to Violence, Abuse and Neglect\*](#).

### 15.2.2 Where access is not authorised by patient

Section 11.2.8 provides detailed guidance on where the [\*Health Records and Information Privacy Act 2002\*](#) allows law enforcement agencies, including the police, to access personal health information. This guidance should be followed where the patient has not consented or has refused to release their information.

### 15.2.3 Search warrant

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



#### Further guidance:

- Section 11.2.8 Law enforcement agencies, including police
- Section 11.3.7 Search warrants and subpoenas

### 15.2.4 Police interviews

#### 15.2.4.1 Interviews with patients

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

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

#### 15.2.4.2 Interviews with patients under the age of 16

If a patient is under the age of 16, a parent or legal guardian should be present during police interviews, unless the circumstances of the matter require that the parent or legal guardian are not informed in which case another responsible adult should be present. Alternatively, where appropriate, a parent or legal guardian can give permission for another person to be there.

Special procedures apply in the case of interviews in child abuse cases. Where a parent/guardian is suspected of sexual assault, see [\*The Joint Child Protection Response Program, local planned response\*](#).

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

#### 15.2.4.3 Interviews with victims of sexual assault

Where police wish to interview the victim-survivor of a sexual assault, the relevant local Sexual Assault Service should be contacted. Police usually take witness statements at police premises, but where appropriate and negotiated in advance a statement may be taken in another safe setting, such as at a sexual assault service.



#### 15.2.4.4 Interviews with staff

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

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



#### Further guidance:

- Section 11.2.3 To prevent a serious and imminent threat to health or welfare
- Section 11.2.8 Law enforcement agencies, including police
- Section 11.3.4 Reporting 'serious criminal offences'

### 15.3 Violence, abuse and neglect

The protection of personal health information is of critical importance for victim-survivors of violence, abuse and neglect. Inappropriate access, use or disclosure of their information can further compromise their safety. Appropriate collection, use and disclosure of health information supports integrated and trauma-informed responses to violence, abuse and neglect both between and beyond health services. This includes ensuring that, when necessary, files can be located by NSW Health services and opportunities for service collaboration can be identified.

Health service policies are in place for the management of information within dedicated Violence, Abuse and Neglect (VAN) services and linkages with other health records systems.

Where health workers identify the need for increased safeguards to protect against inappropriate access and use of a particular person's health information, liaison with Health Information Managers and VAN services assists in mitigating risk. An example of this is where the alleged perpetrator of family violence is a NSW Health worker and could potentially access the survivor's files.

#### 15.3.1 Child Protection Counselling Records

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

- Child Protection Counselling Service records are generally maintained separately from the general health record
- Child Protection Counselling Service records can be linked to the general health record only via a notation that a 'confidential health record exists'
- Access to the content of the record for care and treatment purposes is restricted. Access must be sought via a designated contact in the Child Protection Counselling Service, who in turn will seek patient consent.

#### 15.3.2 Sexual Assault Services and integrated Violence, Abuse and Neglect services

NSW Health has special policies for the records of Sexual Assault Services and integrated Violence, Abuse and Neglect (VAN) Services responding to more than one form of violence, abuse and neglect including sexual assault. In accordance with these policies, integrated VAN Services operate as Sexual Assault Services, and the following applies:

- Sexual Assault Service records are generally maintained separately from the general health record.
- Sexual Assault Service records can be linked to the general health record only via a notation that a 'confidential health record exists' or for an Emergency Department presentation '*Patient presented and disclosed sexual assault. Referred to Sexual Assault Service for review following medical clearance*'.
- Access to the content of the record for care and treatment purposes is restricted. Access must be sought via a designated contact in the Sexual Assault Service, who in turn will seek patient consent.

Counselling records relating to sexual assault may also be subject to sexual assault communications privilege (SACP). See section 15.13.3 on **Sexual Assault Communications Privilege**, which sets how to define, manage and store SACP records.



#### Further guidance:

- [Responding to Sexual Assault \(adult and child\) Policy and Procedures \(PD2020\\_006\)](#)
- [Child Protection Counselling Services Policy and Procedures \(PD2019\\_014\)](#)

- [\*Child Wellbeing and Child Protection Policies and Procedures for NSW Health \(PD2013\\_007\)\*](#)
- [\*NSW Health policy directive 'Subpoenas' \(PD2019\\_001\)\*](#)
- [\*Child Wellbeing and Child Protection – NSW Interagency Guidelines\*](#)
- [\*Legal Aid Subpoena Survival Guide on Sexual Assault Communications Privilege \(SACP\) Service\*](#)
- Section 12.5.3 Department of Communities and Justice
- Section 11.3.7 Search warrants and subpoenas

## 15.4 Health examinations of school children

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

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

Special procedures apply for parental permission for vaccination of school children.



### Further guidance:

- NSW Health [School vaccination program consent materials](#)

## 15.5 Use of interpreters

Patients whose preferred language is a language other than English should be informed in their own language of their rights to access their health records. Similarly, patients who are hearing impaired should have access to an AUSLAN interpreter.

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

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

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

When providing the *Privacy Leaflet for Patients* (see Section 7.4.5), consideration should also be given to giving the patient a translated copy.

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



### Further guidance:

- [\*Interpreters – Standard Procedures for Working with Health Care Interpreters \(PD2017\\_044\)\*](#)
- [\*NSW Health Policy Directive Domestic Violence – Identifying and Responding \(PD2006\\_084\)\*](#)

## 15.6 Legal claims and insurance

### 15.6.1 Claims manager and Treasury Managed Fund

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

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

### 15.6.2 Patient's legal representative

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

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



### Further guidance:

- [\*Health Records and Medical/Clinical Reports – Charging Policy \(PD2006\\_050\)\*](#)
- [\*Health Records and Medical/Clinical Reports – Rates \(IB2019\\_036\)\*](#)

### 15.6.3 Patient's insurer

Where the request is made for information related to an insurance or compensation claim, a photocopy of the insurance application or compensation claim form, signed and dated within the past 12 months by the client/patient, containing the patient's consent to disclosure, is sufficient authority for the release of relevant health records or a summary of injuries (discharge summary).

It will normally be sufficient for the health service to provide a medical report or summary of injuries for such claims to be processed. If further information is requested, only relevant sections of the patient's health record may be provided.

Patient consent is required for disclosure of additional health records.



#### Further guidance:

- Section 11.2.1 Directly related purpose
- Section 11.2.2.1 Where a third party seeks access

### 15.6.4 NSW Motor Accident (Compulsory Third Party 'CTP') Claims

The *Motor Accident Injuries Act 2017* establishes a compensation scheme for people injured in motor accidents in NSW. The legislation promotes rehabilitation and recovery, and insurers are required to proactively support the claimant to optimise their recovery and return to work expeditiously.

Persons injured in a motor accident are entitled to statutory benefits in the form of weekly income support and payment of medical expenses for up to 12 months, regardless of fault. Whether the injured person will receive benefits beyond 12 months will be dependent on whether the injured person was at fault and whether the injuries suffered reach the threshold of severity.

A copy of the consent to disclosure, signed and dated by the patient or representative, is sufficient authority for the release of relevant health records. CTP insurers have agreed to provide this consent document to health services on request. It will normally be sufficient for the health service to provide a medical report or summary of injuries for such claims to be processed. Sometimes additional health information is required to properly manage the rehabilitation of the injured person. If further information is requested, only relevant sections of the patient's health record may be provided.



#### Further guidance:

- [State Insurance Regulatory Agency \(SIRA\) Information Sheet: Invoicing information for NSW Health doctors](#) (patients injured in motor vehicle accidents)

## 15.7 Enquiries about hospital patients, including media

### 15.7.1 Enquiries about patients

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

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

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

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

### 15.7.2 Other safeguards for enquiries sections

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

### 15.7.3 Media queries

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

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

### 15.7.3.1 Responsibility for media liaison

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

### 15.7.3.2 Accident victims

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



#### Further guidance:

- [NSW Health Public Communication Procedures \(PD2017\\_012\)](#)

### 15.7.3.3 Information about health practitioners

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

If information is released to a media agency, only information about health practitioners working for the health service may be released.

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

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

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



#### Further guidance:

- [NSW Health Public Communication Procedures \(PD2017\\_012\)](#)

## 15.8 Fundraising

### 15.8.1 Consent for uses or disclosures for fundraising or publicity purposes

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

Patients have a right to withdraw consent and to have their names and addresses removed from any lists held. Health services should ensure:

- direct mail contains a statement of the addressee's right to have his/her name removed from mailing lists
- correspondence clearly displays the name and full address of the sender
- patients are made aware that if their withdrawal of consent is received after the mailout has been sent, they may receive one final correspondence.

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



#### Further guidance:

- Section 5.4 Consent

### 15.8.2 Use of mailing lists

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

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



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

### 15.8.3 Organisations with a commercial interest

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

## 15.9 Information-specific laws and policies

All personal health information is generally considered to be sensitive personal information, which a patient will generally expect to be shielded from public disclosure. The terms of the [Health Records and Information Privacy Act 2002](#) are based on adopting and reflecting these expectations.

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

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

### 15.9.1 Aboriginal health information

The [Aboriginal Health and Medical Research Council of NSW \(AHMRC\)](#), the peak body representing Aboriginal Community Controlled Medical Services in NSW, developed the [NSW Aboriginal Health Ethics Guidelines: Key Principles](#), to ensure that research impacting Aboriginal people and communities is undertaken in partnership, in a culturally safe way that fully considers those it may affect.

The guidelines provide a framework of ethical and culturally sensitive protocols for the collection and use of personal health information relating to Aboriginal people in NSW.



#### Further guidance:

- [NSW Aboriginal Health Ethics Guidelines: Key Principles](#)
- [Centre for Aboriginal Health, NSW Ministry of Health](#)

### 15.9.2 Adoption information

Any application by a person involved in an adoption for access to adoption-related information (including birth-related information) should be referred to the [Adoption Information Unit, Department of Communities and Justice \(DCJ\)](#).

Where a request is received from a person or organisation other than DCJ, the facility should contact DCJ to establish the bona fides of the inquirer before releasing the information.

To prevent matching of adopted persons or adoptive parents with biological parents in health records, copies of correspondence should be kept physically separate from the biological parents' health records.



#### Further guidance:

- [Adoption Act 2000 – Release of Information \(PD2016\\_036\)](#)

### 15.9.3 Service-based policies

#### 15.9.3.1 Genetics services

Genetic healthcare information collected by NSW Health services often includes a family tree with details that may infer information about the health status of other relatives, sometimes without their knowledge or consent. All genetic healthcare records should be stored securely. Genetic health records are typically kept long-term, as family health tree information can be valuable for genetic relatives including future generations.

#### 15.9.3.2 Third party access – insurers and employers

The results of predictive or pre-symptomatic testing generally relate to healthy people but may indicate risk of developing a disorder in later life. If access to predictive test results is requested by third parties, such as insurers and employers, patient consent must be sought prior to disclosure. There is no obligation on a health practitioner to disclose information to such a third party.



### 15.9.3.3 Third party access – genetic relatives

Where a health practitioner anticipates a situation where information will be obtained from a patient which may be of interest or potential benefit to other family members, he or she should discuss this with the patient prior to treatment being commenced or as part of protocols for ordering tests. Through counselling, individuals should be encouraged to accept their own responsibilities with regard to the information needs and rights of others.

The [Health Records and Information Privacy Act 2002](#) allows for the disclosure of genetic information to genetic relatives without patient consent, albeit in very limited circumstances, in accordance with guidelines issued by the NSW Information and Privacy Commission.



#### Further guidance:

- Section 11.2.3.5 Genetic information
- [NSW Genetic Health Guidelines: Use and disclosure of genetic information to a patient's genetic relatives: Guidelines for organisations in NSW October 2014 \(NSW IPC\)](#)
- [NHMRC Guidelines for Genetic Registers and Associated Genetic Material \(1999\)](#)
- [NHMRC Use and disclosure of genetic information to a patient's genetic relatives under Section 95AA of the Privacy Act 1988 \(Cth\) \(2014\)](#)

### 15.9.3.4 Sexual assault services

Health services have local policies for the management of information collected by NSW Sexual Assault Services. See: 15.3 Violence, Abuse and Neglect.

## 15.9.4 Service-based practices

Policies for dealing with the collection of personal health information by stand-alone drug and alcohol or sexual health services are generally developed at the operational level. Staff should contact the local service for further details on how health records are managed both in hard copy and as electronic health records.

Patients attending these types of stand-alone services will often have expectations about how their information has been used. As a result, many of these services have developed specific practices in the management of the personal health information they collect.



#### Further guidance:

- Section 16 Electronic health information management systems.

### 15.9.4.1 Sexual health services

Some sexual health services are provided as stand-alone services, not integrated into a general hospital, and therefore patients may have the expectation that these records are held separately to any general health records relating to them, and that these records would not be shared with staff outside the health service without their consent. Most sexual health services have policies which rely on extensive patient consents to determine how and when information about the services received by a patient can be disclosed.

Where sexual health service records are part of the District's electronic health record system, auditing which targets access to these records is an appropriate system support for protecting privacy of sensitive information.

Staff should refer to local policies with regards to the management of electronic health records.

In addition, the [Health Records and Information Privacy Act 2002](#) allows for disclosure for emergency purposes (see Section 11.2.3), and with lawful authorisation (see Section 11.3). Other exemptions listed in Section 11 also continue to apply.

Special statutory restrictions are also imposed on access to information about a person's HIV status under the [Public Health Act 2010](#).



#### Further guidance:

- Section 4.1.3 [Public Health Act 2010](#)
- Section 11.2.3.3 [Public Health Act 2010](#) – Notification of public health risk
- Section 15.9.6 Managing public health risks
- Section 16 Electronic health information management systems

## 15.9.5 Organ and tissue donor information

To protect the privacy of grieving relatives of a recently deceased donor, it is not permissible to disclose any information which could enable the identification of the donor of a transplanted organ or tissue.

Issues relating to the disclosure of information in such cases are comprehensively dealt with under section 37 of the [Human Tissue Act 1983](#). Under this provision the identity of the donor and recipient of transplanted tissue (whether living or deceased) must not be disclosed except in the following circumstances:

- with the consent of the person to whom the information relates, or in the case of a deceased person, the authorised representative of the deceased person (see Section 5.6)
- in connection with the administration or execution of the [Human Tissue Act 1983](#)
- in connection with research which has Human Research Ethics Committee (HREC) approval
- for the purposes of any legal proceedings or reporting of such proceedings
- with other lawful excuse.



#### Further guidance:

- [Organ and Tissue Donation, Use and Retention \(PD2022\\_035\)](#)

### 15.9.6 Managing public health risks

The [Public Health Act 2010](#) establishes a range of provisions which impact on the management of personal health information. These provisions ensure the Secretary, NSW Health, has appropriate powers to act when a matter involving risk to public health arises (such as outbreaks of food poisoning or disease).

#### 15.9.6.1 Reporting of certain medical conditions and diseases

The [Public Health Act 2010](#) also establishes requirements for doctors, hospital Chief Executive Officers and laboratories to notify certain diseases to Public Health Units.



#### Further guidance:

- [Notification of Infectious Diseases under the NSW Public Health Act \(IB2013\\_010\)](#)
- [Notifiable Conditions Data Security and Confidentiality \(PD2012\\_047\)](#)
- [NSW Health Infectious diseases](#)
- Section 4.1.5 HIV/AIDS-related information
- [Management of People with HIV Who Risk Infecting Others \(PD2019\\_004\)](#)
- [Tuberculosis Management of People Knowingly Placing Others at Risk of Infection \(PD2015\\_012\)](#)
- [Management of health care workers with a blood borne virus and those doing exposure prone procedures \(PD2019\\_026\)](#)
- [Public Health Act 2010](#)
- [Public Health Regulation 2012](#)

#### 15.9.6.2 Contact tracing

Contact tracing involves informing a person that they may have been at risk of infection because they were in contact with a person with a communicable disease. Decisions in relation to contact tracing are based on a number of factors, including consideration of the risk of exposure and the nature of the disease.

For those conditions followed up by public health units, contact tracing is undertaken confidentially and all efforts are made to protect the identity of the person with the communicable disease. This person is referred to as the 'index case'.

Under clause 61 of the [Public Health Regulation 2022](#), the Secretary, NSW Health (or delegate) or attending medical practitioner may notify a person who is believed to have been in contact with a person suffering from a specified medical condition of measures to be taken (for example, diagnosis, treatment and prevention) to prevent further transmission of infection.

The identity of a contact may be obvious to the person being notified, however, the terms of the regulation still enable contact tracing to proceed. While in such cases the health service involved would not be in breach of patient privacy, the health service should make every effort to protect the identity of the index case wherever this is possible within the scope of contact tracing.

In situations where authorisation has been given for contact tracing without the consent of the index case, it is appropriate for the index case to be informed of this and given a final opportunity to provide consent.



#### Further guidance:

- [Tuberculosis contact investigations \(GL2019\\_003\)](#)
- [Management of People with HIV Who Risk Infecting Others \(PD2019\\_004\)](#)

**Contact:** Local [Sexual Health Clinic](#) or [Public Health Unit](#).

#### 15.9.6.3 Undertaking public health inquiries

Section 106 of the [Public Health Act 2010](#) gives the Secretary, NSW Health (or delegate) broad powers to inquire into any matter relating to the health of the public. A person authorised by the Secretary (or delegate) for the purposes of such an inquiry is entitled to enter premises, inspect and copy health records. These powers can only be exercised where the person has been issued with a Certificate of Authority by the Secretary, NSW Health (or delegate) under section 106 of the Act.

## 15.10 Deceased patients

Privacy law continues to apply to the information of a deceased person for 30 years after their death.

When dealing with the information of deceased persons, a health service should have regard to:

- special provisions allowing disclosure of information for compassionate purposes (see Section 11.2.10)
- other grounds allowing use or disclosure of health information under HPPs 10 and 11
- provisions for access to information held by a health service provided for under the [Government Information \(Public Access\) Act 2009](#)

Any decision to disclose material held on a deceased patient should also have due regard to any view expressed by the patient prior to death, either in writing, or as recorded in the patient's health record. This would include any advanced directive, such as an Advanced Care Directive, made by the patient.



### Further guidance:

- Section 11.2.10 Disclosure on compassionate grounds
- Chapter 12 Patient access and amendment

## 15.11 Virtual Care (Telehealth)

Virtual care image transfer and clinical consultations follow the same privacy rules as face-to-face consultations, and therefore the principles contained in this Manual can be applied to virtual care consultations.

While the same principles apply, clinicians should have clear guidance on how to manage, use and disclose any identifiable patient or third-party images they have access to when using virtual care technologies. Further guidance can be provided by the Privacy Contact Officer or local Virtual Care/Telehealth Manager.

There are circumstances where patients will see a contracted third party for the delivery of virtual care. In some of these circumstances, the personal health information that is collected may be recorded in NSW Health patient records, as well as in external records that NSW Health does not control. Such records may be held by treating clinicians from private practices. Clinicians should inform patients where these circumstances apply.

There may also be circumstances whereby patients are referred to external virtual care services. Referrers should be clear when this applies, and patients should be informed that their personal

health information will not be managed by NSW Health.

Written consent to receive a virtual care service is only required if consent is normally required for face-to-face sessions or for research. If a virtual care session is to be conducted as part of a research activity, a research ethics application will determine and provide approved documentation.

Video or sound recordings of virtual care consultations generally should not be made, in the same way that such recordings are generally not made for face-to-face consultations. If it is proposed that a consultation be recorded, verbal or written patient consent must be obtained and documented in the record. Recordings which capture personal health information are subject to strict storage and retention rules as set out in the [State Records Act 1998](#) and the [Health Records and Information Privacy Act 2002](#) (see Section 9 Retention, security and protection (HPP 5)).

Documentation requirements for virtual care are the same as for in-person care. A patient's health record should be updated at all points of care, including the modality used and the participant details. If virtual consultations take place while the clinician is in the field, patient information must be documented and transmitted using an approved secure platform. Consult the Health Information Manager for advice on local procedures and policies.

Guidance on the use of telehealth when working with victim-survivors of violence, abuse and neglect is available from the NSW Health [Violence, abuse and neglect and telehealth](#) webpage.



### Further guidance:

- [ACI Virtual Care Team](#), NSW Agency for Clinical Innovation (ACI)
- [ACI Virtual Care in Practice](#)
- [Ministry of Health Virtual Care Resources](#)
- Section 9.2.3.3 Messaging and Collaboration tools
- Section 9.2.2 Images, photography

## 15.11A Recording online meetings involving patient health information

To minimise privacy risks, online meetings involving discussion of health information should not generally be recorded unless there is a strong justification. Before choosing to record meetings that may include discussion of identified patient health information, health organisations must ensure there is a legitimate purpose for doing so. Recording meetings

merely because the functionality is available may result in the unnecessary collection of health information and other sensitive or confidential information. If a case conference is recorded for note taking purposes, the recording must be deleted as soon as the minutes are finalised.

Meeting recordings may be considered 'State Records' under the [State Records Act 1998](#). Therefore, local business rules should be developed for the management of these recordings consistent with [State Records Act 1998](#) requirements.

Care should be taken in relation to any recorded meetings related to patient care. Relevant health information, including any decisions made in the meeting regarding diagnosis, treatment and clinical management, must be maintained in patient records. Recordings of discussions between clinicians related to a patient's care should not be stored separately from the patient record. The discussion should be documented in the patient record and the recording should be deleted or retained as an electronic file in the patient record.

Care will also need to be taken with any identifiable patient images to ensure they are not used or disclosed outside the clinical purpose and that they are stored and deleted appropriately.

In the case of meetings where a patient's health information is discussed for other purposes, such as quality assurance or clinical supervision, different considerations apply. In many cases, recordings will not need to be retained once minutes are finalised and should be permanently deleted. Recordings of significant discussions that are not separately documented may need to be retained as State records in the relevant records management system.

If participants want to distribute the recording outside the meeting group, the meeting host should be contacted for advice on consent, where the use or disclosure is not otherwise lawfully authorised.

Staff should also be aware that they have obligations under the [Surveillance Devices Act 2007](#) and covert recordings can only be used legally in very limited circumstances.

Users must be notified that a meeting will be recorded prior to the event. This provides participants time to express any reasonable objections and for the convenor of the meeting to confirm the confidentiality obligations of the meeting if any patient images or medical records are being shared.

Users should also be offered alternative ways to participate in the meeting if they do not want to be recorded.

This might include allowing the use of the audio function in a meeting, so participants are not videoed; or allowing use of the mute function if participants would prefer to comment via the chat function.

Staff names may still appear as participants in the recorded meeting group (even if sound is muted and video is off) but this information is generally not regarded as personal information (see Section 12.3.1.1).



#### Further guidance:

- Section 9.2.3.3 Collaboration tools
- Section 15.11 Virtual care (Telehealth)
- [NSW Health Video Conferencing Platforms Guideline](#)

## 15.12 Community health records

### 15.12.1 Group houses/hostels

Comprehensive health records of patients residing in group houses or hostels should continue to be maintained and securely stored.

The non-institutional nature of group houses and hostels present challenges for managing the privacy of health information and special precautions should be taken to ensure that patient privacy is maintained.

Health records should be stored in a secure place, inaccessible to patients and visitors. Health records maintained and kept at the home/hostel should be limited to:

- registration book: content may vary but should include identification data and referrals accepted and refused
- daybook
- card index or mini file: should include identification data, referral information and medication details.

### 15.12.2 Group sessions

Individual patient intake forms (or equivalent) should be placed behind a chart divider to separate them from the group form and protect the privacy of each patient or there should be an electronic alternative to securing the different records.

### 15.12.3 Family consultations

In the case of family consultations, information on other family members may be recorded in the health record of the family member who is the patient. Extreme care should be taken to safeguard the privacy of other family members.

Information about family members, or other third parties, which the patient (or person seeking access



to the health record) may be unaware of, must not be disclosed without consent from that individual.

Where multiple family members are patients of the health service, family records must be maintained as individual records.

Where release of information on an individual has been appropriately authorised, care should be taken to ensure that only information relating to the specific episode indicated by the individual patient is released.

In circumstances where access is sought for information relating to group sessions and the participants consent has not been obtained, a GIPA application would be the most appropriate way to manage such a request. However, this does not guarantee access to the information. The agency will need to consider the application, and where appropriate consult with any third parties if practicable, so that any relevant public interest considerations for and against disclosure can be determined.



#### Further guidance:

- Section 11.2.3.5 Genetic information
- Section 15.9.3.1 Genetics services
- [Client Registration Policy \(PD2007\\_094\)](#)
- See Section 4.2.2 [Government Information \(Public Access\) Act 2009](#)

## 15.13 Maintaining the health record

This section is designed to provide guidance on key obligations in managing the health record. It is the responsibility of the record keeper to ensure compliance with those provisions of the [Health Records and Information Privacy Act 2002](#), and this Manual which apply to health records. Also refer to Section 9, and Section 16 of this Manual.

Clearly visible privacy notices should be attached to health records or flagged in electronic systems.

### 15.13.1 Quality of health records

The health record should comply with the security requirements of Section 9 of this Manual and be sufficiently detailed and comprehensive to:

- provide effective communication to health care providers
- provide for a patient's effective, ongoing care
- enable evaluation of the patient's progress and health outcome
- retain its integrity over time.

Because the primary purpose of keeping health records is to enable better patient care, it is important that the information in health records is current, clear, accurate, complete and readily available.

A number of documentation models exist, and practices may vary according to local needs. Whatever model or method is used, the health record should be clear and comprehensible to others.

### 15.13.2 Accuracy and completeness

To ensure that the health record is accurate and complete:

- information should be recorded at the time of consultation or procedure or as soon as it becomes available
- entries should generally be made by those collecting the information or present when the information was collected
- each entry should be signed by the clinician, their designation, the date and time clearly legible; electronic signatures must be managed with care to ensure equivalent accuracy is maintained
- alterations or deletions should not be made; original incorrect entries should not be erased but lined through so the original entry remains readable, and such action should be explained and signed
- the senior treating health practitioner should periodically review the health record for correctness
- there should be an audit trail for electronic health records.



#### Further guidance:

- Section 10 Accuracy
- Section 16.3.4 Auditing
- [Health Care Records – Documentation and Management \(PD2012\\_069\)](#)
- [NSW Health Patient Matters Manual](#), Section 9

### 15.13.3 Control of health records

Control over the movement of health records is of the utmost importance. An adequate health record tracking system, tailored to local needs, is essential to facilitate prompt record location and ensure that patient care does not suffer, and privacy is not breached.

Systems for transporting health records within a health service should be well supervised to ensure that health records are not accessible by unauthorised persons.



No health record should be removed from its home location without the following details being recorded in an appropriate system:

- health record number
- patient name
- destination/location of the health record
- person responsible for/in possession of the health record or, data custodian for the paper or electronic health record system where the record has been relocated
- date health record was removed

Records subject to the Sexual Assault Communications Privilege should be marked confidential and transported in sealed envelopes or other secure electronic file systems.

Similar principles apply to the movement of electronic record systems. Appropriate checks and governance should ensure that electronic systems are secure and managed to prevent any inappropriate access during any transfer of information. Also, that information does not remain accessible after it has been removed.

eHealth NSW's approved [secure file transfer \(SFT\)](#) software for all NSW health organisations is available on the eHealth NSW intranet. It should be used where sending and/or transferring patient health information.



#### **Further guidance:**

- [NSW Health Electronic Information Security Policy Directive \(PD2020\\_046\)](#)
- [Communications – Use & Management of Misuse of NSW Health Communications Systems \(PD2009\\_076\)](#)
- [Health Care Records – Documentation and Management \(PD2012\\_069\)](#)
- Section 9.2.4 Secure File Transfer (SFT) and other systems

### **15.13.4 Removal**

Health records should be kept under adequate security as outlined in Section 9 of this Manual and the original only removed from the control of the health service upon receipt of a court subpoena, summons, statutory authority, search warrant, or a coronial subpoena or notice to produce (see Chapter 9 of the Patient Matters Manual) or by order of the Secretary, NSW Health.

Whenever the original health record leaves a health service, a copy of that record should, where possible, be made beforehand and kept.

### **15.13.5 Transfer**

If it is necessary to transfer a paper-based health record outside the health service it should be transferred under seal, marked 'confidential' and where possible sent by courier.

Where health records are transported by staff members, for example as part of a Community Health Service, care must be taken to ensure records are not in public view and should be securely transported in a closed non-transparent container.

It is the responsibility of the staff member who receives the health record to ensure it is kept in a secure location to prevent loss and unauthorised access. A register should be kept of the records showing when and to whom they are released and returned.

Electronic transfer of health records must also be secure. Health services should not transfer electronic health records by posting data stored on a USB stick. Health services should consider the use of [secure file transfer](#) software approved by eHealth NSW for this purpose.



#### **Further guidance:**

- Section 9.2.4 Safeguards when delivering and transmitting information
- Section 9.2.4 Secure File Transfer (SFT) and other systems

### **15.13.6 Storage, archiving and disposal**

Disposal of health records should comply with Section 9.1 of this Manual and the [State Records Act 1998](#) and take into account the type of information contained in a health record and possible future demand for it as well as the needs of individual health services. The following should be considered:

- use of health records for patient care, medico-legal purposes, research and teaching
- archival value
- provisions of the [Evidence Act 1995](#) and the Statute of Limitations ([Limitations Act 1969](#), including for example that there is no limitation period for child abuse damages claims)
- available storage space
- requirements under the provisions of the [State Records Act 1998](#).

Similar standards for maintaining privacy and security should be maintained for health records in

archival or secondary storage as for health records in current use.



#### Further guidance:

- [\*Health Care Records – Documentation and Management \(PD2012\\_069\)\*](#)
- [\*Patient Matters Manual\*](#) Section 9
- [\*GDA-17-General Retention and Disposal Authority Public health services: patient/client records\*](#)

### 15.13.7 Health facility closures

When a facility is closed and ceases to operate, each responsible unit should create a register that includes details of:

- health records destroyed
- health records retained
- health records transferred to other locations
- location(s) where the health records have been transferred to
- officers who undertook closures

The full name of the facility being closed and the facility receiving the records should be clear on the register, along with the date of closure, the date range of records destroyed, the date range of records transferred and the range of medical record numbers if possible.

Details of records that are to be destroyed should include, as a minimum:

- the location where the health records were created
- the patient's surname and given name
- the patient's sex
- the patient's date of birth
- the last date of contact with the facility
- the general nature of the health records
- the date for destruction or the date destroyed.

## 15.14 NSW data collections

### 15.14.1 NSW Health data

Statistical information and other data are submitted to the Ministry of Health for inclusion in a number of centrally maintained data collections. Collection of such data is required or authorised by a range of health legislation, such as the [\*Public Health Act 2010\*](#), the [\*Health Administration Act 1982\*](#), the [\*Private Health Facilities Act 2007\*](#), and the [\*Home and Community Care Act 1985 \(Cth\)\*](#).

### 15.14.2 Health Information Resources Directory (HIRD)

Central data collections and the data elements they contain are documented in the Health Information Resources Directory (HIRD). The HIRD is the authoritative central registry for data collections and metadata. It is the responsibility of each data custodian, or other delegate of the data sponsor, to ensure that the data collection for which he or she is responsible, if in scope, is recorded in HIRD.

Health services that also own or administer data collections should also keep a register of those collections. Such a register should include (as a minimum):

- data collection name
- collection sponsor
- collection custodian and contact details
- statement of the collection's purpose
- any Act or Regulation authorising the collection
- statement of whether the collection includes personal health information.

### 15.14.3 Staff roles

All staff employed within the health system have a duty to maintain, within their roles, the privacy, integrity and security of data held and managed by their work unit.

**Data sponsor:** Each data collection has a nominated data sponsor who undertakes the duties of ownership on behalf of the relevant health service, including:

- defining the purpose of the data collection
- establishing the scope and coverage of the collection
- defining access and custody arrangements.

**Data custodian:** The data sponsor appoints a custodian for each data collection who is responsible for:

- data storage and disposal
- compliance of data with relevant legislation and policies
- administration
- quality assurance
- data access and release.

For further guidance, contact your organisation's [\*Privacy Contact Officer\*](#).

### 15.14.4 Access to data collections

Where data collections contain identifying or potentially identifying information, HPPs 10 and 11

will apply to any requests for use and access. While access may be authorised under any of the exceptions listed in HPP 11(1) and 11(2), the most common are likely to be where:

- the access relates to the primary purpose for which the data was collected (for more detail, see Section 11.1)
- the access is for a directly related purpose, which would be 'reasonably expected' by the individual (see Section 11.2.1)
- the access is required or authorised by law (see Section 11.3)
- use or disclosure is required for management or research purposes (see Section 11.2.5).

Where access is sought for research or management purposes, the NSW Privacy Commissioner's [Statutory Guidelines](#) on research and management apply. These guidelines provide for requests for such access to be approved by a Human Research Ethics Committee (HREC). In relation to data collections held by the NSW Ministry of Health, applications should be made to the [NSW Population and Health Services Research Ethics Committee](#) (NSW PHSREC).

Based on the evaluation report of the PHSREC or another HREC, the appropriate data custodian will approve or reject the request and advise applicants in writing of the committee's recommendation, including reasons for denial of access and any conditions or constraints.

An exception to this may be in circumstances where the research project also includes non-NSW Health data. NSW Health organisations may not be able to require NSW PHSREC approval as the National Mutual Acceptance (NMA) is a national system for mutual acceptance of scientific and ethical review of multi-centre human research projects conducted in publicly funded health services across jurisdictions.

The scope of NMA includes any form of human research as defined in the [National Statement on Ethical Conduct in Human Research](#) (NHMRC, 2007) for which an application must be made to a Human Research Ethics Committee (HREC).

#### 15.14.4.1 Conditions of access

If access is granted, the principal applicant must sign an agreement to apply, as a minimum, the standards of privacy protection contained in the [Health Records and Information Privacy Act 2002](#), and to abide by any other conditions or constraints (relating to charges and monitoring requirements) on the use of the data set by the data custodian.

Although NSW Health strive to facilitate access to data by bona fide applicants, access is not

guaranteed. Each request will be judged, and access granted or denied, on its own merits. The information supplied will always be the minimum required to meet a project's objectives and requirements.

Access, when granted, should be subject to the terms and conditions set out in an agreement, to be drawn up by the data custodian and signed by the principal applicant. If access is refused, the reasons for refusal should be documented in a written response from the data custodian. The applicant may choose to amend the proposal in the light of this response and re-submit it, in which case the assessment process will need to be repeated.



#### Further guidance:

- [NSW Health Data Governance Framework \(GL2019\\_002\)](#)
- [Disclosure of unit record data by Local Health Districts for research or contractor services \(PD2018\\_001\)](#)
- [NSW Enforceable Procurement Provisions](#)
- [NSW Health Procurement \(PD2022\\_020\)](#)
- [Office of the National Data Commissioner](#)
- [Data Availability and Transparency Act 2022](#)

#### 15.14.4.2 Record linkage

Linkage of specific data is authorised under the [Health Records and Information Privacy Act 2002](#), provided the linkage is necessary for the purposes of management or research and the [Statutory Guidelines](#) have been complied with. Linkage of data may also occur where otherwise legally permitted, such as under the public health register provisions in the Public Health Act 2010.

Linkage of whole health records for the purposes of establishing an ongoing health record must, however, comply with HPP 15.

#### 15.14.4.3 NSW Population and Health Services Research Ethics Committee

The [NSW Population and Health Services Research Ethics Committee](#) (NSW PHSREC) is constituted as a Human Research Ethics Committee (HREC) in accordance with NHMRC guidelines for the protection of privacy in the conduct of medical research. The committee undertakes assessment of requests for access to personal information held in data collections maintained at central administration. The PHSREC also considers:

- proposals for data use or issues requiring ethical advice referred by NSW Ministry of Health officers
- multi-centre research proposals

- proposals referred by HRECs
- proposals for data and health record linkage.

## 15.15 Artificial Intelligence (AI) and Privacy

AI is the ability of a computer system to perform tasks that would normally require human intelligence, such as learning, reasoning, and making decisions. Generative AI tools, a subset of AI, can produce novel content such as text, images, audio, video, and code in response to prompts, presenting new and innovative opportunities for healthcare. While generative AI models and AI tools more broadly have unique and powerful capabilities, many use cases can present significant privacy risks for individuals.

### Privacy risks when using AI tools

The use of personal information in AI systems is a source of significant community concern and this is particularly heightened when health and other sensitive information is being handled. While some uses of AI are low-risk, others may present a major privacy risk. Where NSW Health seeks to use any form of AI, a cautious approach should be adopted, it is necessary to understand how the tool uses information and privacy risks should be considered upfront.

The Health Privacy Principles within the [Health Records and Information Act 2002 \(HRIP Act\)](#) apply when handling health information in any AI tools. Improper use of AI tools can result in data loss, privacy breaches, and the perpetuation of biases present in the data the tool was trained on.

Guidance on AI in this Manual does not cover all privacy issues and obligations in relation to the use of AI, and should be considered together with the Information Protection Principles and Health Privacy Principles outlined in the PPIP Act and [HRIP Act](#), as well as all relevant NSW Health policies

### Privacy best practices when using AI tools

Personal or health information, and particularly sensitive information, should not be entered into publicly available AI chatbots and other publicly available generative AI tools. Any information entered into these tools are outside the control of NSW Health and is likely to be a privacy breach.

Be mindful of the risk of data aggregation, which occurs when individual pieces of information combine to reveal classified, personal, or sensitive data. Never enter information that, when combined with previous inputs, could inadvertently expose such data. Even minor details can accumulate to form a

comprehensive picture that could be extrapolated by AI tools.

Inherent bias can exist within data and algorithms used in AI applications and any AI outputs need to be assessed carefully for accuracy, fairness, and suitability before using them.

Remember that any use of an AI tool which generates or infers new personal information about an individual is considered an additional 'collection' of personal information and must comply with the Health Privacy Principles 1-4 relating to collection.

### Examples of appropriate and inappropriate usage of AI tools

Appropriate case uses:

- Brainstorming and finessing ideas for an upcoming seminar or event
- Summarising a publicly available article or document
- Drafting an engaging out of office message.

Inappropriate case uses:

- Entering sensitive, personal or confidential information to generate content e.g. a patient's name and medical details
- Sharing commercially sensitive documents
- Inputting data that is not publicly available.

For more information and guidance around responsible Gen AI use, please read:

- [The NSW Government basic guidance on Generative AI \(for all public sector staff\)](#)
- [Advice on the use of Generative Artificial Intelligence \[IB2024\\_059\]\(for NSW Health\).](#)



# 16 Electronic health information management systems

The continued expansion and growth in digital technologies is aiding the development of many new electronic health information management systems to improve efficiency and quality of care within NSW Health.

Electronic health information management systems require robust security and governance policy and practices in place to maintain the integrity of the data and the trust of the people of NSW.

Such policies assist staff compliance with their privacy obligations and reduce the risk of privacy and security breaches through effective communication and management processes (see Section 14.4 Breach of Health Privacy Principle(s) by an employee).

The fundamental principles for management of, and access to, electronic health information management systems are provided below (see Section 16.3 Fundamental principles). These principles should be incorporated into local security and governance practices in order to maximise the benefits of electronic health information management systems and minimise the privacy and security risks.

When new electronic health information systems are being planned and designed, they should be subject to Privacy Impact Assessments (PIAs) to ensure privacy considerations have been addressed. This is particularly important where new technologies are to be introduced that impact treatment arrangements, for example, remote patient monitoring or use of vendor platforms to manage clinical images.

Health information about an individual must not be included in a health records linkage system unless express consent has been obtained. Exemptions exist where an entity may be lawfully authorised, or not required to comply. This extends to where the inclusion of the record falls under an exemption under HPP 10(1)(f) or HPP 11(1)(f).



## Further guidance:

- [IPC Guide to Privacy Impact Assessments](#)

## 16.1 Electronic health records

Electronic health records differ from paper health records in ways that warrant special consideration. Firstly, it is possible to have a single electronic health

record simultaneously accessible at multiple sites, giving more people access. Secondly, it is possible to control access to an electronic health record in ways that are not possible with a paper health record.

Health records in relation to a particular patient may consist of both hard copy (paper) and electronic health records (sometimes referred to as a *hybrid* record). When handling personal health information, it is important to consider whether relevant health information is held in the other format and whether both the electronic health record and the hard copy health record need review when making a decision about the health information contained in the records.

Electronic records may also include data collected for remote patient monitoring and data collected by vendor systems engaged for patient care purposes. Those arrangements will be subject to contractual arrangements that manage the access and security of health records, like any NSW health record.

## 16.2 Data collections and data warehousing

Data collections and data warehousing systems are subject to the [Health Records and Information Privacy Act 2002](#) and therefore Health Privacy Principles 10 and 11 regarding use and disclosure of personal health information will apply (see Section 11 Using & disclosing personal health information (HPPs 10 & 11)). There are a range of reasons why NSW Health will establish data collections, including:

- provision of clinical care to patients and in some circumstances their families
- public health surveillance
- performance monitoring
- service management and improvement
- service planning and policy development
- allocation of funds
- public accountability
- research in accordance with guidelines by the NHMRC (see Section 11.2.5 Management, training or research).

Health Privacy Principles 10 and 11 allow for the above uses of personal health information as they fall into the definition of a 'directly related purpose' (see Section 11.2.1 Directly related purpose) or meet the criteria for a management or research activity

(see Section 11.2.5 Management, training or research).

NSW Health data collections can often be based on statistical or other data and so may not include 'identifiable' information. Where identifiable information is not included, privacy laws do not apply (see Section 16.2.1 Identified and de-identified data).

### 16.2.1 Identified and de-identified data

Within some NSW Health data collections, data may be classified in various ways such as: fully identified data, semi-identified data, re-identifiable data and de-identified data.

For example, data can be classified as:

- Fully identifiable: required for patient care purposes and other secondary purposes
- Partially identifiable: may be used for management purposes, for example to group cardiac patients by condition, postcode, age group or sex for various management purpose including waiting lists, ward requirements, surgical access etc.
- Re-identifiable: this might be for hospital or ward operational reporting and will not identify an individual unless linked with other data (for example, date of surgery, hospital, address may be re-identifiable)
- Un-identified / fully deidentified: for certain research purposes and has been carefully stripped of all identifiers.

Whilst these may be valid and useful classifications for management of information, they are not used in the privacy laws. When considering the implications under privacy law for the access, use or disclosure of health information held in any context within NSW Health, regard needs to be had to the definitions of 'personal health information' used in the [Health Records and Information Privacy Act 2002](#). These provide that 'information about an individual whose identity is apparent or can reasonably be ascertained from the information' is personal information and therefore regulated by the [Health Records and Information Privacy Act 2002](#).

If there is a reasonable chance that the information is potentially identifiable, it will fall within the ambit of the privacy law controls, unless it is otherwise lawfully exempt.

Clearly, whether information can be considered de-identified will be dependent on the specific circumstances which arise in any disclosure.

Privacy laws and policies only apply to identified data (also see Sections 5.1 Health information, and 5.2 Personal information).



#### Further guidance:

- Section 5.3 De-identified information
- [De-Identification Decision-Making Framework](#), OAIC and the CSIRO
- [Fact sheet: de-identification of personal information](#), Information and Privacy Commission (IPC)
- [Privacy issues and the reporting of small numbers](#), HealthStats NSW, NSW Health

## 16.3 Fundamental principles

Electronic systems facilitate access to personal health information. Staff and health providers should be aware of their obligation to restrict access to what is clinically necessary for patient care, or otherwise authorised under the law. Systems to audit user access and protect security to ensure compliance with these obligations should be in place.

The following principles provide guidance on how to address privacy issues when accessing electronic health information management systems, such as electronic health records, NSW Health data collections, and data warehousing systems.

### 16.3.1 Privacy and confidentiality undertakings for staff

Staff who have access to electronic health information management systems (eMRs) must sign a [NSW Health Privacy Undertaking](#) on employment and when gaining access to each eMR and other systems, outlining their responsibility to observe the Health Privacy Principles and duties of confidentiality.

A [NSW Health Privacy Undertaking](#) must be signed where staff, contractors, vendors and others are provided with extended or project access to health information management systems or other sensitive information in their employment.

The [NSW Health Privacy Undertaking](#) reminds staff about their obligations when accessing and using personal and health information in their day-to-day work.

### 16.3.2 Training and informing staff

Staff accessing electronic health information management systems must be informed and regularly reminded of their responsibilities in relation to patient privacy and confidentiality. This can be achieved through a combination of staff induction, staff meetings, training, staff newsletters, notices (including pop-up reminders in electronic systems) and posters.

Providing staff with brief privacy messages at critical decision points in the system may be an effective way of reminding staff of privacy obligations.

See section 6.1.4 Staff communication and alerts, for examples of electronic notifications for NSW Health staff about privacy obligations.



#### Further guidance:

- Section 6.1.2 Staff training
- Section 14 Complaints handling

### 16.3.3 Access protocols

The approval process for access applications to electronic health information management systems should have robust governance systems to minimise opportunities for inappropriate use and disclosure. Features of robust access protocols include:

- Access to electronic health information management systems should be provided on a 'needs only' basis. Consideration should be given as to whether access to de-identified data, or limited identified data, is sufficient for the staff member's work requirements.
- Where access to identifiable data is required, the purpose/business requirement should be documented as part of the access application.
- Access should be specific to job requirements or for the duration of a project, and then reviewed/renewed at appropriate intervals, depending on the business needs.
- Staff (and any other users) who are provided with access to any system containing personal health information should have a secure individual login which should not be shared. Health organisations should have processes in place to discourage the sharing of passwords. Sharing passwords significantly decreases security controls and exposes the health information to unauthorised access, use and disclosure. Generic passwords should only be used for systems which contain de-identified information, generally used for analysis and reporting.
- Robust processes must be in place for regular review of access arrangements for individuals, for example, where staff move into a new role access levels should be reviewed and if staff leave the organisation their logins to all systems, including remote access functionality, should be disabled.

- Clear criteria for approval for access to an electronic health information management system must be followed and documented, for example:
  - confirmation of each applicant's employment status and position
  - the name of each system to which access is to be provided and the associated level of access to be provided
  - confirmation that the application has been approved by the Line Manager
  - confirmation that each applicant/manager has provided requirements for access
  - confirmation that if access is for a specific project, the requested time period for access is appropriate to meet business needs and liaison with system administrators will occur to ensure access is reviewed as approved.

### 16.3.4 Auditing

Audit functionality is a mechanism which can be incorporated into electronic health information management systems holding personal health information.

Data quality which includes the completeness and accuracy of health information (both demographic and clinical) is an important principle in the management of health information (HPP 9). As part of audit functionality, electronic health information systems should have control mechanisms that assess and report on data quality.

Audit records of access to health records should be maintained on an ongoing basis. Audit reports and notifications should be generated regarding access to health records as required. Systems should be in place to appropriately manage security and minimise unauthorised breaches of access.

Key elements that support a robust audit process may include:

- The ability to run an audit report which identifies the name and ID of the user, their position/designation, and the name of the patient (and MRN) of the record accessed.
- The ability of any audit report to set out the time when access to a record commenced and ceased, and parts of the record that were accessed.
- Reminders to staff that audits are proactively conducted to promote privacy awareness and compliance. This might include auditing access to a VIP hospital attendance (politician, celebrity etc.) or a random patient sample.
- A protocol for managing privacy audits and potential staff breaches with appropriate thresholds for disciplinary referral.

Audit functionality may include:

- Creation of an audit record each time a user accesses, creates, updates or archives personal health information via the system.
- A log which uniquely identifies the user, the data subject (the patient), the function performed by the user, and the time and date at which the function was performed.
- When a record is updated, a record of the original data, who entered the new data, and the time and date, should be retained.
- A log of message transmissions containing personal health information.

The organisation should carefully assess and determine the retention period for these audit logs, with particular reference to clinical professional standard and legal obligations, in order to enable investigations to be carried out when necessary.

### 16.3.5 Informing patients

Patients should be made generally aware that their personal health information will be managed using electronic systems, and that systems are in place to prevent unauthorised access to information held in these systems. This is included in the [Privacy Leaflet for Patient](#).



#### Further guidance:

- Section 9.2.3 Computer systems and applications
- Section 11 Using & disclosing personal health information (HPPs 10 & 11)

## 16.4 [Evidence Act 1995](#)

The [Evidence Act 1995](#) does not preclude electronic records being used as evidence unless their veracity can be questioned. To minimise the possibility of records converted from paper being open to challenge, the equipment and scanning processes must be capable of scanning to 100% accuracy with no possibility of corruption or manipulation of images. Control processes should be implemented to ensure that images cannot be altered between scanning and storage or while stored. Scanning processes should include quality control checking mechanisms to ensure the captured image is legible and reproducible.

## 16.5 Accountability

Information accountability means that the use of information should be transparent, so it is possible to determine whether a particular use is appropriate and in accordance with the 15 Health Privacy Principles, and that the system enables individuals and health services to be held accountable for any misuse of information.

Accountabilities should be clearly articulated for the system which delivers the record to ensure the integrity of electronic health records. Backup and recovery solutions are required in case of disaster.

Whoever enters the information into the health record is accountable for the accuracy of the information. Some staff will have additional responsibility for ensuring the overall accuracy of the health record and the care with which the details have been documented.

## 16.6 Access and quality control

The area over which the electronic health record is available is important, for example, individual facility, campus or health service. The broader the system, the greater the need for tighter network and access controls.

Where the electronic health record system covers multiple facilities, the health records may contain a mix of entries from different sources or partial copies of health records from other facilities. The ability to maintain a single, logical health record in this situation is critical. This can be achieved through various means such as individual patient identifiers, employee numbers, appropriate labeling of each transaction and adequate version control. Identification and authentication of the person making the entry is important.

Electronic health records should are to meet the same records documentation quality standards and requirements as paper records, for example, when clinical inaccuracies are identified in the health record, the inaccurate data should not be deleted. The original data must be retained as a contemporaneous record, flagged that it has been identified as inaccurate and the amendment entered as a dated notation, making the record complete and accurate. This is different from corrections (or updates) that may relate to changes in demographic data, for example, or information that has been incorrectly attached to the wrong patient's record (where to retain the information in the wrong electronic record could potentially breach patient privacy). Governance processes should be in place to manage the different clinical requirements for the management of errors and amendments.



## 16.7 Patient access

It is important to ensure that the right of patients to access their own health records is not compromised by the introduction of electronic health records. Health facilities should have local policies, compliant with privacy obligations which allow patients access to their health records. Technologies in some circumstances allow some patient-facing capabilities, for example portals and smart phone applications, which allow patients to view subsets of their own information.

Electronic health records should be retained in compliance with the *GDA-17-General Retention and Disposal Authority Public health services: patient/client records*. Fees and charges raised for access to health information should be consistent with NSW Health policy.

Adequate viewing, printing and copying facilities should be readily available. All requests for access to health information must be in accordance with Health Privacy Principles 6 and 7 (see Section 12 Patient access and amendment).

## 16.8 My Health Record

NSW Health services have access to the My Health Record system via HealtheNet, subject to access controls that may be set by the patient. The *My Health Records Act 2012 (Cth)*, regulates most aspects of My Health Record. NSW Health organisations are subject to mandatory data breach notification requirements for breaches relating to the My Health Record. Health services are required to notify the Australian Digital Health Agency of data breaches involving My Health Record.

### 16.8.1 Mandatory security and access requirements

All health services must ensure that their local processes comply with the Policy Directive *My Health Record Security and Access (PD2019\_054)* in relation to the following:

- Information security, privacy, and access controls must be in place.
- Access to the My Health Record System for NSW Health purposes must only occur through NSW Health's HealtheNet Clinical Portal.
- Access to My Health Record is auditable via HealtheNet.
- Districts are strongly encouraged to maintain records of the individuals who have access to and/or received training to access the My Health Record system.
- If a patient requests that documents relating to a particular episode of care not be uploaded to My Health Record, the documents must not be uploaded.



#### Further guidance:

- *My Health Record Security and Access (PD2019\_054)*
- *Office of the Australian Information Commissioner, 'Guide to mandatory data breach notification in the My Health Record system'*
- Section 11 Using & disclosing personal health information (HPPs 10 & 11)
- Section 13.3 Linkage of health records (HPP 15)
- *NSW Health Electronic Information Security Policy Directive (PD2020\_046)*
- *Health Care Records – Documentation and Management (PD2012\_069)*

# Index

\*References in **bold** denote the principal reference.

## A

Aboriginal health information	<a href="#">Section 15.9.1</a>
Access	
Access to health records by patients	<a href="#">Section 4.2.2</a> , <a href="#">Section 9.2.1.2</a> , <b>Section 12</b>
Access to health records by staff	<a href="#">Section 3.1 and 3.3</a> , <b>Section 9</b> , <b>Section 9.2.3</b> , <a href="#">Section 11</a> , <a href="#">Section 15.14</a> , <a href="#">Section 16</a>
Access to health records by VMOs, MOs	<a href="#">Section 12.5.4</a>
Access to health records of correctional centre inmates	<a href="#">Section 11.3.3</a>
Access to health records of minors	<a href="#">Section 5.5.2</a>
Access to health records by a patient's authorised representative	<b>Section 5.6</b> , <a href="#">Section 12</a>
Access to health records by third parties	<a href="#">Section 11.2.2.2</a> , <b>Section 12</b> , <a href="#">Section 15.1</a> , <a href="#">Section 15.9.3.2</a> , <a href="#">Section 15.9.3.3</a> , <a href="#">Section 15.12.3</a>
Access to health records by contracted agencies	<b>Section 6.4</b>
Access to health records by researchers, students	<a href="#">Section 11.2.5</a>
Access to health records, Auditing of	<a href="#">Section 16.3.4</a>
Accident victims	<a href="#">Section 15.7.3.2</a>
Accuracy of personal health information	
Summary of accuracy principle	<a href="#">Section 2.2</a> , <b>Section 10</b>
Checking the accuracy of patient information prior to electronic transmission	<a href="#">Section 9.2.4.6</a>
Maintain the accuracy of health records when providing access	<a href="#">Section 12.3.1.4</a>
Where changes to a health record do not meet the requirements for accuracy	<a href="#">Section 12.8.2</a>
Check the accuracy of a patient's GP details	<a href="#">Section 15.1.5</a>
Maintaining accuracy of the health record	<a href="#">Section 15.13.2</a>
Staff responsibility for accuracy	<b>Section 10</b> , <a href="#">Section 16.5</a>
Accredited chaplain	
Defined	<a href="#">Section 1</a>
Privacy Manual applies to Accredited chaplains	<a href="#">Section 3.1</a>
Services of an accredited chaplain considered a health service	<a href="#">Section 5.1</a>
Chaplaincy services provided by accredited chaplains	<a href="#">Section 1</a> , <b>Section 11.2.10</b>
Acronyms	<a href="#">Section 1</a>
Additions to health records	<a href="#">Section 12.8</a>
Admission and registration forms for patients	<b>Section 7.4.4</b> , <a href="#">Section 10</a> , <a href="#">Section 11.1</a> , <a href="#">Section 15.1.5</a>
Adoption information	<a href="#">Section 15.9.2</a>
AIDS, See HIV-related information	
Alcohol and drug services, See Drug and Alcohol services	
Alias, use of	<a href="#">Section 8.3</a>
Alterations to health records	<a href="#">Section 10</a> , <b>Section 12.8.1</b> , <a href="#">Section 15.13.2</a>

Ambulance Service of NSW	<a href="#">Section 1</a> , <a href="#">Section 3.1</a>
Amendments to health records	<a href="#">Section 2.2</a> , <a href="#">Section 10</a> , <a href="#">Section 12.8</a>
Annual reporting, privacy	<a href="#">Section 6.1.1</a> , <a href="#">Section 6.7</a>
Anonymity for patients	<a href="#">Section 3.5</a> , <a href="#">Section 8</a> , <a href="#">Section 8.3</a> , <a href="#">Section 9.2.6</a> , <a href="#">Section 11.2.5.2</a>
Apprehended Violence Orders	<a href="#">Section 12.5.2</a>
Archiving of health records	<a href="#">Section 9.1</a> , <a href="#">Section 15.13.6</a>
Auditors, disclosure to	<a href="#">Section 3.1</a> , <a href="#">Section 11.2.1.1</a>
Australia, transferring information out of	<a href="#">Section 11.2.3.1</a> , <a href="#">Section 13.2.2</a>
Authorised representatives	<a href="#">Section 5.6</a>
Collection of health information from an authorised representative	<a href="#">Section 7.3</a> , <a href="#">Section 7.4</a> , <a href="#">Section 7.4.14</a>
Disclosure of health information to an authorised representative	<a href="#">Section 9.2.1.2</a>
Accuracy of details for an authorised representative	<a href="#">Section 9.2.4.6</a> , <a href="#">Section 10</a>
Authorised representative to consent on behalf of patient	<a href="#">Section 11.2.2.1</a> , <a href="#">Section 12.3.1.4</a> , <a href="#">Section 15.1.6</a>
Authorised representative to consent on behalf of deceased patient	<a href="#">Section 11.2.9</a> , <a href="#">Section 15.9.5</a>
<b>B</b>	
Breach of privacy	
General principles	<a href="#">Section 14.1</a>
Sanctions for	<a href="#">Section 14.2</a>
Notifying individuals of a breach of their privacy	<a href="#">Section 14.3</a>
By an employee	<a href="#">Section 14.4</a>
<b>C</b>	
Capacity	
Test for capacity	<a href="#">Section 5.5</a>
Determining capacity for minors	<a href="#">Section 5.5.2</a>
Where the patient lacks capacity	<a href="#">Section 5.6</a> , <a href="#">Section 7.3</a> , <a href="#">Section 7.4.1.1</a> , <a href="#">Section 11.2.2</a>
Certificate of expert evidence	<a href="#">Section 11.2.8.3</a>
Chaplaincy and pastoral care services	<a href="#">Section 1</a> , <a href="#">Section 11.2.10</a>
Charges for access to health records	<a href="#">Section 12.7</a>
Chief Executives	<a href="#">Section 1</a> , <a href="#">Section 6.1</a>
Application of Privacy Manual to	<a href="#">Section 3.1</a>
Privacy annual reporting	<a href="#">Section 6.7</a>
Public Interest Disclosures	<a href="#">Section 11.2.7.1</a>
Public Health Risk reporting	<a href="#">Section 15.9.6</a>
Chief Health Officer	<a href="#">Section 4</a>
Child Death Review Team	<a href="#">Section 11.3.11</a>
Child protection, disclosure of records for	<a href="#">Section 11.3.2</a>
Child protection records, management of	<a href="#">Section 12.5.3</a> , <a href="#">Section 12.5.3</a> , <a href="#">Section 15.3.1</a>
Child sexual assault services	<a href="#">Section 15.3.2</a>
Children	
Capacity to consent	<a href="#">Section 5.5.2</a>
Information requests from parents	<a href="#">Section 5.5.2</a> , <a href="#">Section 5.6.1.1</a> , <a href="#">Section 12.3.1.3</a> , <a href="#">Section 12.5.1</a>
In Out of Home Care (OOHC)	<a href="#">Section 5.6.1</a>
School health examinations	<a href="#">Section 15.4</a>

<a href="#"><i>Children and Young Persons (Care and Protection) Act 1998</i></a>	<a href="#">Section 4.1.6</a> , <a href="#">Section 11.3.2</a> , <a href="#">Section 12.5.3</a>
Claims managers, disclosure of health information to	<a href="#">Section 11.2.1.1</a> , <a href="#">Section 15.6.1</a>
Clinical images, See Images of patients	
Clients, See Patients	
Clinical placements	<a href="#">Section 9.2.6</a> , <a href="#">Section 11.2.5.2</a>
<a href="#">NSW Health Code of Conduct (PD2015_049)</a>	<b><a href="#">Section 4.3.2</a></b> , <a href="#">Section 9.2.2</a>
Collection of personal health information	<a href="#">Section 7</a>
Common law	<a href="#">Section 4.3</a>
Commonwealth agencies	<a href="#">Section 11.3.14</a>
Communications between clinicians, See also Verbal communications, Conversations	<b><a href="#">Section 9.2</a></b> , <a href="#">Section 9.2.7</a> , <a href="#">Section 10</a> , <a href="#">Section 11</a>
Telehealth communications	<a href="#">Section 15.11</a>
<a href="#">Privacy Act (Cth) 1988</a>	<a href="#">Section 4.1.8</a> , <a href="#">Section 13.2.1</a>
NHMRC guidelines under the <a href="#">Privacy Act (Cth)</a>	<a href="#">Section 11.2.5.2</a>
Community health records	<a href="#">Section 15.12</a>
Community Services Department, See Family and Community Services (FACS)	
Compassionate grounds for disclosure	<b><a href="#">Section 11.2.9</a></b> , <a href="#">Section 12.4</a> , <a href="#">Section 11.2.2</a>
Disclosure of genetic information	<a href="#">Section 11.2.3.5</a>
Third party access on compassionate grounds	<a href="#">Section 11.2.9</a>
Compensation claims, See Insurance and Compensation	
Complaint handling	<a href="#">Section 14</a>
Access to health information by VMOs, Mos to respond to a complaint	<a href="#">Section 12.5.4</a>
Completeness of health records	<b><a href="#">Section 10</a></b> , <a href="#">Section 15.13.2</a> , <a href="#">Section 16.3.4</a>
Additions and corrections to a health record, importance of completeness (HPPs 8 & 9)	<a href="#">Section 2.2</a> , <a href="#">Section 10</a> , <b><a href="#">Section 12.8</a></b>
Collection of health information, importance of completeness	<a href="#">Section 7.2</a>
Compliance tips	<a href="#">Section 6.5</a>
Computer systems	<a href="#">Section 9.2.3</a>
Computer screen displays, securing	<a href="#">Section 9.2.8</a>
Computerised health records, See Electronic records	
Confidentiality agreements, See Privacy undertakings	
Confidentiality duties, See Duties of confidentiality	
Consent, See also Express consent	
Principles of consent	<a href="#">Section 1</a> , <b><a href="#">Section 5.4</a></b> , <a href="#">Section 11</a>
Where a person lacks capacity to consent	<a href="#">Section 5.5</a> , <a href="#">Section 5.6</a>
Patient consent for a third party to access health records	<a href="#">Section 9.2.1.2</a> , <b><a href="#">Section 11.2.2</a></b> , <a href="#">Section 12.3.1.1</a> , <a href="#">Section 12.4</a>
Consent for disclosure to law enforcement agency, Police	<b><a href="#">Section 11.2.8</a></b> , <a href="#">Section 15.2</a>
Patient consent for a use or disclosure of health information by the health service	<b><a href="#">Section 11.2.2.2</a></b> , <a href="#">Section 15.1.6</a>
Patient consent for use of clinical imagery	<a href="#">Section 9.2.2</a>
Patient consent for use of health information for training and presentations	<a href="#">Section 9.2.6</a>



Disclosure of genetic information without consent	<a href="#">Section 11.2.3.5</a>
Consideration of consent for management, training and research activities	<a href="#">Section 11.2.5.1</a>
Consent required for disclosure of patient's names to Ex-service organisations	<a href="#">Section 11.3.14.2</a>
Consent required for release of health information to the media	<a href="#">Section 15.7.3</a>
Consent required for release of health information for fundraising purposes	<a href="#">Section 11.1</a>
Verbal consent	<b><a href="#">Section 11.2.2.1</a></b> , <a href="#">Section 7.4.1.2</a>
Contact tracing for infectious diseases	<a href="#">Section 15.9.6.2</a>
Contracted agencies	<a href="#">Section 6.4</a>
Control of health records	<a href="#">Section 15.13.3</a>
Conversations, discretion in	<a href="#">Section 9.2.7</a>
Copying health records	<a href="#">Section 9.2.5</a>
Correctional health centre inmates, access to records	<a href="#">Section 11.3.3</a>
Coroner, authority to access health records	<a href="#">Section 11.3.6</a>
Corrections to health records, <i>See</i> Amendments to health records	
Crime, obligations to disclose, <i>See also</i> Law enforcement agencies	<a href="#">Section 11.3.4</a>
<i>Crimes Act</i>	<a href="#">Section 11.3.4</a>
<b>D</b>	
Data collections	<a href="#">Section 15.14</a> , <a href="#">Section 16.2</a>
Data sponsors and custodians	<a href="#">Section 15.14</a>
De-identified information	<b><a href="#">Section 5.3</a></b> , <a href="#">Section 11.2.5.1</a> , <a href="#">Section 16.2.1</a> , <a href="#">Section 16.3.3</a>
Deceased patient records	<a href="#">Section 15.10</a>
access to	<a href="#">Section 12</a>
Definitions	<a href="#">Section 1</a>
Demonstrations, <i>See</i> Training	
Department of Family and Community Services (Clth)	<a href="#">Section 11.3.2</a>
Department of Health (NSW), <i>See</i> Ministry of Health (NSW)	
Department of Immigration and Border Protection (Clth)	<a href="#">Section 11.3.14.3</a>
Department of Veterans' Affairs	<a href="#">Section 11.3.14.2</a>
Digital equipment, use of	<a href="#">Section 9.2.3</a>
Digital images, <i>See</i> Images of patients	
Directly related purposes	<a href="#">Section 11.2.1.1</a>
Director-General of NSW Health, <i>See</i> Secretary of NSW Health	
Discharge referrals and summaries	<a href="#">Section 15.1.5</a>
Transmission of	<a href="#">Section 9.2.4.6</a>
Disciplinary policies for misconduct	<a href="#">Section 11.2.7</a> , <a href="#">Section 11.3.15</a>
Disclosure of personal health information	<a href="#">Section 2.2</a> , <a href="#">Section 4.1</a> , <a href="#">Section 4.3</a> , <b><a href="#">Section 11</a></b>

Disclosure of 'sensitive' information, *also see*  
Sensitive information

On compassionate grounds

Mandatory disclosure under the

*Government Information (Public Access) Act 2009*

Disclosure outside of NSW

Disguised identity, *See* Alias

Disposal of health records

Divorced parents seeking access to records of  
minors

Drug and alcohol services

Duties of confidentiality

## E

eDRS, *See* Electronic records

eHealth

National eHealth Record

*EHR*, *See* Electronic records

Electronic records

Electronic Health Records (EHR)

Information systems management

Linkage of

Privacy undertaking for

Security of

Emergency circumstances- 'stage of emergency'

Use of non-approved digital equipment

To prevent a serious and imminent threat

Law enforcement requests

Email, transmission of records via

Enquiries about patients

Environmental Health Officers

Epidemiological data, release by Chief Health  
Officer

Ethics Committees

*Evidence Act 1995*

Certificates of expert evidence

Expectations of patients

Express consent

To waive right to information

To linkage of electronic health records

## F

Facsimile machine, information transmitted by

Family and Community Services (FACS) (NSW)

Adoption information requests

Child protection reports to

Children in Out-of-homecare in the care of the  
Minister for FACS

Section 5.8

Section 11.2.9

Section 12.2, 12.3

Section 13.2.2

Section 4.2.1, Section 9.1, Section 9.2, Section 15.13.6

**Section 5.6.1.2**, Section 12

Section 3.1, Section 5.8.1, **Section 15.9**

**Section 4.3.1**, Section 4.4, Section 14.1, Section 16.3.1

Section 13.1, 11.3.7, 15.11

Section 16.8

### Section 16

Section 5.4.3, **Section 13.3**, Section 16.3, Section 16.8

Section 6.3.4, Section 9, **Section 16**

Section 13.3

Section 16.3.2

Section 9.2.3, Section 16

Section **11.2.8.5**

Section 9.2.2

Section 11.2.3

Section 11.2.7.5

Section 9.2.4.7

Section 15.7.1, 8.3

Section 11.3.1

Section 4.1.4

Section 15.14.4.3

Section 16.4

Section 11.2.8.3

Section 5.8, Section 7.4.5, **Section 11.2.1**, Section 15.9

Section 7.4.1.2

Section 13.3

Section 9.2.4.4

Section 15.9.2

Section 11.3.2, Section 12.5.3

Section 5.6.1, Section 11.3.2

## Family members

Definition of 'immediate family member'	<a href="#">Section 1</a>
Collection of health information from	<a href="#">Section 7.3</a>
Access to genetic information of	<a href="#">Section 11.2.3.5</a>
Consultations with	<a href="#">Section 15.12.3</a>
Information access by	<a href="#">Section 11.2.2</a> , <a href="#">Section 11.2.9</a> , <a href="#">Section 12.4</a>
Records of a patient's family members	<a href="#">Section 15.1.6</a>
Federal Police, See Law enforcement agencies	
Fees and charges for information access	<a href="#">Section 11.2.2.1</a> , <a href="#">Section 12.7</a> , <a href="#">Section 16.7</a>
Fiduciary duties	<a href="#">Section 4.3.1</a>
Framework, See Privacy framework	
Fundraising, limits on disclosure of records for	<a href="#">Section 11.1</a> , <a href="#">Section 11.2.2.2</a> , <b>Section 15.8</b>

## G

General Disposal Authority	<a href="#">Section 9.1</a>
Transfer of General Practice records	<a href="#">Section 15.13.7</a>
For electronic records	<a href="#">Section 16.7</a>
Genetic information	<a href="#">Section 11.2.3.5</a>
Definition of	<a href="#">Section 5.1</a> , <a href="#">Section 5.2</a>
Deciding whether consent is required for disclosure of	<a href="#">Section 5.4.4</a> , <a href="#">Section 11.2.3.4</a> , <a href="#">Section 15.9.3.3</a>
Record keeping of	<a href="#">Section 15.9.3.1</a>
GIPA Act	<a href="#">Section 4.2.2</a> , <a href="#">Section 12.2</a>
<i>Government Information (Public Access) Act 2009</i>	<a href="#">Section 4.2.2</a> , <a href="#">Section 12.2</a>
General Practitioner (GP)	
Consent not required for referral to	<a href="#">Section 5.4.4</a>
Accuracy of GP details	<a href="#">Section 10</a>
Disclosure of health information, referrals to	<a href="#">Section 9.2.4.5</a> , <a href="#">Section 11.2.1</a> , <a href="#">Section 15.1.1</a> , <a href="#">Section 15.1.5</a>
Transfer of GP records to a health service	<a href="#">Section 15.13.7</a>
Group sessions, records of	<a href="#">Section 15.12.2</a>
Guardian	
Enduring guardian	<a href="#">Section 1</a> , <a href="#">Section 5.6</a>
Legal guardian for minors	<a href="#">Section 5.5.2</a> , <a href="#">Section 15.2.4.2</a>
Person responsible	<a href="#">Section 5.6</a>

## H

<i>Health Administration Act 1982</i>	<a href="#">Section 4.1.1</a>
Health Care Complaints Commission	
powers of	<a href="#">Section 11.2.7</a>
Information to be provided to	<a href="#">Section 11.2.7</a> , <a href="#">Section 11.3.8</a> , <a href="#">Section 15.13.7</a>
Health facility closures	
Health information	
Definition of	<a href="#">Section 5.1</a>
Privacy legislation relating to	<a href="#">Section 2.1</a> , <a href="#">Section 4.1</a>
Health Privacy Principles (HPPs) relating to	<a href="#">Section 2.2</a>
Privacy Manual covers	<a href="#">Section 3.3</a>
'Sensitive' health information	<a href="#">Section 5.8</a>
Held in electronic management systems	<a href="#">Section 16</a>
Health Information Resources Directory (HIRD)	<a href="#">Section 15.14.2</a>
Health Information Service (HIS)	

Definition of	<a href="#">Section 1</a>
Staff to be aware of	<a href="#">Section 6.3</a>
Consultation with HIS in regard to	
Authorised representative	<a href="#">Section 5.6</a>
Access to health records	<a href="#">Section 9.2.1.2</a> , <a href="#">Section 9.2.2</a> , <b>Section 12.2</b>
Disclosure of health records	<b>Section 11</b> , <a href="#">Section 11.2.8</a> , <a href="#">Section 11.3.15</a>
Health Practitioner Regulation National Law (NSW)	<a href="#">Section 4.3.3</a>
Health, preventing a serious and imminent threat to	<a href="#">Section 4.3.1</a> , <b>Section 11.2.3</b>
Disclosure for law enforcement	<a href="#">Section 11.2.7.5</a>
Disclosure outside Australia	<a href="#">Section 13.2.2</a>
Health Privacy Principles, overview of	<a href="#">Section 2.2</a>
HPP 1: purposes of collection	<a href="#">Section 7.1</a>
HPP 2: how to collect	<a href="#">Section 7.2</a>
HPP 3: who to collect from	<a href="#">Section 7.3</a>
HPP 4: individual to be made aware of collection	<a href="#">Section 7.4</a>
HPP 5: retention and security	<a href="#">Section 9</a> , <a href="#">Section 16</a>
HPP 6: information held by organisations	<a href="#">Section 12</a>
HPP 7: access to information	<a href="#">Section 12</a>
HPP 8: amendment of information	<a href="#">Section 12</a>
HPP 9: accuracy	<a href="#">Section 10</a>
HPP 10 & HPP 11: use and disclosure	<a href="#">Section 11</a>
HPP 12: identifiers	<a href="#">Section 13</a>
HPP 13: anonymity of information	<a href="#">Section 8</a>
HPP 14: transmittal outside NSW	<a href="#">Section 13</a>
HPP 15: linkage of records	<a href="#">Section 13</a>
<i>Health Practitioner Regulation National Law (NSW)</i>	<a href="#">Section 4.3.3</a>
Health professionals,	<a href="#">Section 3.1</a> , <a href="#">Section 4.3.2</a>
Also see <a href="#">Staff</a>	
Reporting misconduct of	<a href="#">Section 11.2.7</a> , <a href="#">Section 11.3.15</a>
Health professional registration	<a href="#">Section 4.3.3</a>
Health record	
Access by family members	<a href="#">Section 11.2.9</a> , <a href="#">Section 12</a>
Access by third parties	<a href="#">Section 11.2.2.1</a>
Access to data collections	<a href="#">Section 15.14.4</a>
Amendment by patients	<a href="#">Section 12.8</a>
In group houses/ hostels	<a href="#">Section 15.12.1</a>
Linkage of	<a href="#">Section 13.3</a> , <a href="#">Section 15.14.4.2</a>
Pro forma privacy notice for	<a href="#">Section 7.4.5</a>
Storage and maintenance of	<a href="#">Section 9</a>
Use and disclosure of	<a href="#">Section 11</a>
<a href="#">Health Records and Information Privacy Act 2002</a>	<a href="#">Section 2.1</a> , <a href="#">Section 3.3</a>
Health service staff, See <a href="#">Staff</a>	
Health service, seeks to use or disclose health information	<a href="#">Section 11</a>
<a href="#">Health Services Act 1997</a>	
Statutory reporting requirements under the	<a href="#">Section 7.1</a> , <a href="#">Section 11.3.15</a>
HIRD (Health Information Resources Directory)	<a href="#">Section 11.3.13</a>
HIV-related information, See also <a href="#">Sexual health services</a>	<a href="#">Section 15.14.2</a>
	<b>Section 4.1.5</b> , <a href="#">Section 5.8</a> , <a href="#">Section 11.2.3.3</a> , <a href="#">Section 12.3.1.1</a>

HPPs, See Health Privacy Principles  
HRECs, See Human Research Ethics Committees  
HRIP Act, See [Health Records and Information Privacy Act 2002](#)  
Human Research Ethics Committees, also see PHSREC

Defined	<a href="#">Section 1</a>
Approval for use of organ and tissue donor information	<a href="#">Section 15.9.5</a>
Approval for access to NSW data collections	Section 15.14.4
Approval for management, training and research activities	Section 11.2.5

<b>I</b>	
Identifiers assigned to individuals	Section 13.1
Images of patients	<b><a href="#">Section 9.2.2</a></b> , Section 16.4
Immigration and Border Protection, Department (Clth)	<a href="#">Section 11.3.14.3</a>
Implied consent	Section 5.4.2
Incapacity	<a href="#">Section 5.5</a>
Indigenous Australians, See Aboriginal health information	
Infectious diseases, obligations regarding	<a href="#">Section 15.9.6</a>
Information, See Personal health information; Health records	
Information systems, See also electronic records	Section 6.3.4
Security of	Section 9, Section 16
Management of	Section 16
Auditing of	<a href="#">Section 16.3.4</a>
Information technology department	Section 6.3.4
Consultation with	<a href="#">Section 9.2.2</a>
Informed consent	<a href="#">Section 5.4</a>
Use of interpreters and	Section 15.5
Insurance and compensation	
Documents required for claims	<a href="#">Section 12.4</a> , Section 12.5.4, <b>Section 15.6</b>
Information required for	<a href="#">Section 11.2.2</a>
Workcover claims	Section 11.3.12
International transfers of information	Section 13.2
Interpreters, use of	Section 15.5
Interstate transfer of information	Section 13.2
Interviews with police	Section 15.2.4
Investigations of misconduct	<a href="#">Section 11.2.7</a>
Investigative agencies	<a href="#">Section 11.2.8</a>

<b>J</b>	
Justice Health and Forensic Mental Health Network (Justice Health NSW), prison officers	<a href="#">Section 11.3.3</a>
Justice Health and Forensic Mental Health Network (Justice Health NSW), <a href="#">NSW Health – NSW Police Force Memorandum of Understanding 2018</a> and guidelines	<a href="#">Section 11.3.3</a>



## K

Kids & Families NSW

[Section 11.3.2](#)

Key concepts

Section 5

## L

Law enforcement agencies, *See also* Crime

[Section 11.2.8](#)

Legal claims, information required for

Section 12.5.4, Section 15.6

Legal representatives of patients, *See also*

[Section 5.6](#), [Section 11.2.2.1](#), [Section 12.4](#), **Section 15.6.2**

Authorised representative

Legislation, *See* Common law, names of Acts,

Privacy laws

Linkage of health records

Section 13.3

## M

Mail, information transmitted by

Section 9.2.4.4

Mailing lists, removal of details from

Section 15.8, Section 15.8.2

Management of health services, use of health information in

Section 11.2.5

Media enquiries about patients

[Section 15.7.3](#)

Medical practitioners, *See* Health practitioners, Staff, GPs

Medical research, *See* Research

[Mental Health Act 2007](#)

Section 4.1.2

[Migration Act 1958 \(Cth\)](#), powers to obtain information under

[Section 11.3.14.3](#)

Minister for Health, information required by

Section 11.3.16.1

Ministerial correspondence and briefings

Section 11.3.16.1

Ministry of Health (NSW)

Privacy Contact Officer for

Section 6.2

Privacy annual report provided to

[Section 6.7](#)

Notification of privacy complaint to

[Section 14](#)

Media enquiries directed to

[Section 15.7.3](#)

Data collections managed by

[Section 15.14](#)

NSW Population and Health Services Research

Section 15.14.4.3

Ethics Committee (PHSREC)

Ministry of Health officers

Privacy Contact Officer for NSW Ministry of Health

Section 6.2

Powers to obtain information

Section 11.3.1

Minors, *See* Children

Misconduct, use of records to investigate

[Section 11.2.7](#)

Missing persons, location of

Section 11.2.6

Mobile phone use, *See* Smart phone use

My Health Record

[Section 1](#), **Section 16.8**

## N

Next of kin

Section 5.6.1.3

Non-government organisations

Bound by this Manual

[Section 3.1](#)

Bound by Commonwealth legislation

Section 4.1.9

Contracted agencies

[Section 6.4](#)

Notifiable diseases, obligation to report	Section 11.2.3.3
NSW Civil & Administrative Tribunal (NCAT)	<a href="#">Section 14.3</a>
NSW data collections	<a href="#">Section 15.14</a> , <a href="#">Section 16.2</a>
NSW Health data	<a href="#">Section 15.14</a> , <a href="#">Section 16.2</a>
NSW Health privacy webpage	Section 6.6
NSW Kids & Families	<a href="#">Section 11.3.2</a>
NSW Privacy Commissioner	Section 6.2, <a href="#">Section 7.4.1.4</a> , <a href="#">Section 9.2.6</a> , <a href="#">Section 11.2.3.5</a> , <a href="#">Section 11.2.5</a> , <a href="#">Section 11.2.5.2</a> , <b><a href="#">Section 14.4</a></b> , <a href="#">Section 15.4.4</a>
<i>Also see <a href="#">Statutory Guidelines</a> issued by the NSW Privacy Commissioner</i>	
NSW, transferring information out of	Section 13.2
<b>O</b>	
Official visitors, powers of	Section 11.3.10
Ombudsman	
Powers of	Section 11.3.9
As an investigative agency	<a href="#">Section 11.2.8</a>
In child death review	<a href="#">Section 11.3.11</a>
Ongoing care	
Deciding whether consent is required for	Section 5.4.4, <a href="#">Section 11.2.2.1</a>
Impracticable to provide anonymous health service for	<a href="#">Section 8.1</a>
Electronic documents for	<a href="#">Section 9.2.4.6</a> , <a href="#">Section 16</a>
Use and disclosure of health information for	<b>Section 11.2.1</b>
Providing health information to GPs and other third parties for	<b><a href="#">Section 11.2.1.1</a></b> , <a href="#">15.1</a>
Out of home care (OOHC), children in	<a href="#">Section 11.3.2</a>
<b>P</b>	
Paper health records,	
Security of	<a href="#">Section 6.4</a> , <b>Section 9.2.1</b>
Transfer of	<a href="#">Section 15.13.5</a>
Parents and guardians	
As authorised representatives	<a href="#">Section 5.6</a>
Divorced, <i>See</i> Divorced parents	
Parenting orders	<a href="#">Section 5.6.1.2</a> , <a href="#">Section 12.5.1</a>
Requests for information by	<b>Section 5.6.1.2</b> , <a href="#">Section 12</a>
Pastoral care services, <i>See</i> Chaplaincy	
Patient journey boards, <i>See</i> Whiteboards	
Patients	
Access to information	<a href="#">Section 12</a>
Admission and registration forms for	<b>Section 7.4</b> , <a href="#">Section 10</a> , <a href="#">Section 11.1</a>
Anonymity rights	<a href="#">Section 8</a>
Electronic records of	<a href="#">Section 9.2</a> , <a href="#">Section 13.3</a> , <a href="#">Section 16</a>
Enquiries about	<a href="#">Section 15.7</a>
Expectations of	<a href="#">Section 5.8</a> , <a href="#">Section 11.2.1.2</a>
Legal representatives	<a href="#">Section 5.6</a> , <a href="#">Section 11.2.2.1</a> , <a href="#">Section 12.4</a> , <b>Section 15.6.2</b>
Obligations to inform	<a href="#">Section 7.4</a>
Privacy of charts	<a href="#">Section 9.2.1.2</a>
Reasonable expectations of	<a href="#">Section 5.8</a> , <b>Section 11.2.1.2</b> , <a href="#">Section 11.2.10</a>
Rights to privacy	<b>Section 3.5</b> , <a href="#">Section 4.3</a> , <a href="#">Section 6</a> , <a href="#">Section 7.4</a> , <a href="#">Section 12</a>

Personal affairs, information affecting	<a href="#">Section 7.2</a> , <b><a href="#">Section 12.3.1.1</a></b>
Personal information	<a href="#">Section 5.2</a>
Personal health information, <i>See also</i> Health records	<a href="#">Section 5.1</a>
'Persons responsible', <i>See</i> Authorised representative	
Photocopying	<a href="#">Section 9.2.5</a>
PHSREC, <i>See</i> Population and Health Services Research Ethics Committee (NSW)	
<a href="#">Poisons and Therapeutic Goods Act 1966</a>	<a href="#">Section 11.3.15</a>
Police, <i>See also</i> Crime	<a href="#">Section 11.2.7</a> , <a href="#">Section 15.2</a>
Population and Health Services Research Ethics Committee (NSW)	<a href="#">Section 15.14.4.3</a>
Portable media	<a href="#">Section 9.2.3</a>
Power of attorney	<a href="#">Section 1</a> , <a href="#">Section 5.6</a>
PPIP Act, <i>See</i> <a href="#">Privacy and Personal Information Protection Act 1998</a>	<a href="#">Section 2.1</a>
Practitioners, <i>See</i> Health professionals	
Premier, information required by	<a href="#">Section 11.3.16</a>
Primary purpose, use and disclosure for	<a href="#">Section 11.1</a>
Printing of records	<a href="#">Section 9.2.5</a>
Prison officers, access to prisoners' records	<a href="#">Section 11.3.3</a>
<a href="#">Privacy Act (Cth) 1988</a>	<a href="#">Section 4.1.8</a>
<a href="#">Privacy and Personal Information Protection Act 1998</a>	<a href="#">Section 2.1</a> , <a href="#">Section 3.4</a> , <a href="#">Section 3.8</a> , <a href="#">Section 5.2</a>
Privacy Contact Officers	<a href="#">Section 6.2</a>
Privacy framework	<a href="#">Section 3.8</a>
Privacy issues	
Common privacy issues	<a href="#">Section 15</a>
Consent based privacy issues	<a href="#">Section 5.4</a>
Staff awareness of	<a href="#">Section 6.1.2</a>
Complaints relating to	<a href="#">Section 14</a>
Privacy laws	<b><a href="#">Section 2.1</a></b>
Responsibilities under	<a href="#">Section 6</a>
Use and disclosure authorised by	<a href="#">Section 11</a>
<a href="#">Privacy Leaflet for Patients</a>	<a href="#">Section 7.4.5</a>
Privacy poster	
Generic	<a href="#">Section 7.4.6</a>
Youth friendly	<a href="#">Section 7.4.7</a>
Private organisations, <i>See</i> Non-government organisations	
Professional obligations	<a href="#">Section 4.3</a> , <a href="#">Section 15.1.2</a>
Proof of identity	<a href="#">Section 11.2.2</a> , <b><a href="#">Section 12.6</a></b>
Protection of health records, <i>See</i> Security of health information	
<a href="#">Public Health Act 2010</a>	
Notification of public health risk	<a href="#">Section 11.2.3.3</a>
On HIV disclosure	<a href="#">Section 4.1.5</a>
Statutory reporting requirements	<a href="#">Section 11.3.15</a>

Public health and safety	
Disclosure in the interests of	Section 11.2.3
Inquiries into	Section 15.9.6.3
Managing risks to	<a href="#">Section 15.9.6</a>
Public health units	Section 11.3.1
Public interest disclosures, <a href="#">Public Interest Disclosures Act 1994</a>	<a href="#">Section 11.2.7.1</a>
<b>Q</b>	
Quality assessors, disclosure to	<a href="#">Section 11.2.1.1</a>
Quality of health records	<b>Section 15.13</b> , Section 15.13.1, <a href="#">Section 16.3.4</a> , Section 16.6
<b>R</b>	
Reasonable expectations about information use	Section 5.4.4, Section 5.8, <b>Section 11.2.1.2</b> , Section 11.2.10
Reasonableness, defined	Section 5.2, Section 5.4.4, <b>Section 5.7</b> , Section 5.8
Records, <i>See</i> Health records	
Registered health professionals	Section 4.3.3
Registration of patients, <i>See</i> Admission and registration of patients	
Removal of records	Section 9, <b>Section 15.13</b>
Reporting misconduct, <i>See</i> Misconduct	
Research,	
Use and disclosure of health information permitted for	Section 11.2.1, <b>Section 11.2</b>
Integrity of data for	Section 3.6
Release of epidemiological data for	Section 4.1.4
Research services considered a ‘health service’	<a href="#">Section 5.1</a>
Collection of health information for	Section 7.1
When research activities may be considered a directly related purpose	<a href="#">Section 11.2.1.1</a>
Linkage of health records permitted for	<b>Section 13.3</b> , Section 15.14.4.2
Access to data collections for	<b>Section 15.14.4</b> , <a href="#">Section 16.2</a>
Responsibilities under privacy law	<b>Section 6</b> , Section 15.13, Section 16.3.2, Section 16.5
Summary of	Section 3.8
To inform patients of how they can expect their health information to be handled	Section 7.4.4
To maintain accuracy of health records	<a href="#">Section 10</a>
Confidentiality	Section 4.3.1, Section 16.3.1
Retention of records	Section 4.2.1, Section 9, <b>Section 9.1</b>
Risk of harm	
Disclosure of health information to prevent a risk of harm	Section 11.2.3
Children and young people at risk of harm	<a href="#">Section 11.3.2</a>
Disclosure of health information may expose a person to a risk of harm	Section 12.3.1

## S

Sanctions for breach of privacy	<a href="#">Section 14.2</a>
School children, <i>See</i> Children	
Scope of this manual	Section 3
Search warrants	<b>Section 11.3.7</b> , Section 15.2.3
Secondary purpose, use and disclosure for	Section 11.2
Secrecy provisions	Section 4.1.1
Secretary of NSW Health	
may release research data	Section 4.1.1
HIV-related information disclosed to the	Section 4.1.5
public health and safety inquiries	<b>Section 15.9.6</b> , Section 15.9.6.3
Security of health information	<b>Section 9</b> , <a href="#">Section 15.13.6</a> , Section 15.14.3, Section 16
Obligations under <a href="#">NSW Health Code of Conduct (PD2015_049)</a>	<a href="#">Section 4.3.2</a>
Responsibility of staff to maintain	Section 6
Agreement for contractual agencies to maintain	<a href="#">Section 6.4</a>
Breach of	<a href="#">Section 14</a>
Security of electronic health records	Section 16
Sensitive information	
Definition of	Section 3.4, <b>Section 5.8</b>
Obligation to protect	Section 4.4, Section 11.2.1, <b>Section 16.3.1</b>
Serious criminal offences, <i>See also</i> Law enforcement agencies	<a href="#">Section 11.3.4</a>
Service-based policies and practices	Section 15.9
Sexual assault services	
Interviews with police	Section 15.2.4
Management of records	<a href="#">Section 11.3.2</a> , <a href="#">Section 15.3.1</a> , <a href="#">Section 15.13.3</a>
Policies for information management	<a href="#">Section 15.3.2</a>
Child sexual assault services	<a href="#">Section 15.3.2</a>
Reporting sexual assault	<a href="#">Section 11.3.4</a>
Sexual health service, <i>See also</i> HIV-related information	Section 15.9.4.1
Smart phone use	<a href="#">Section 9.2.2</a> .
SMS, use of	Section 9.2.4.2
Social media, use of	<a href="#">Section 9.2.2</a>
<a href="#">Social Security (Administration) Act 1999 (Cth)</a>	Section 11.3.14.1
Staff, <i>See also</i> Health professionals	
Anonymity rights of	Section 8, <a href="#">Section 11.3.2</a> , <a href="#">Section 12</a>
Bound by this manual	Section 3
Interviews with police	Section 15.2.4.4
Privacy undertakings	<a href="#">Section 6.5</a> , Section 16.3.1
Release of information about	<a href="#">Section 11.3.2</a> , <a href="#">Section 12</a>
Responsibilities under privacy law	Section 3, <b>Section 6</b> , Section 15.13, 16.3.2, Section 16.5
Sanctions against disclosure by	<a href="#">Section 14</a>
Training for	Section 6.1.2, Section 16.3.2
State Police, <i>See</i> Law enforcement agencies	
<a href="#">State Records Act 1998</a>	Section 4.2.1, <b>Section 9</b> , <a href="#">Section 15.13.6</a>
<a href="#">Statutory Guidelines</a> issued by the NSW Privacy Commissioner	<b>Section 11.2.5.2</b>



Third party collection of health information	Section 7.4.1
Use of health information for training activities	<a href="#">Section 9.2.6</a> , <a href="#">Section 11.2.5</a>
Use and disclosure of genetic information	<a href="#">Section 11.2.3.5</a>
Management, training and research activities	Section 11.2.5
Storage of records	<a href="#">Section 15.13.6</a>
Statutory reporting requirements	<a href="#">Section 11.3.15</a>
Students	
Bound by the Manual	<a href="#">Section 3.1</a>
Sharing health information with	Section 11.2.1, <b>Section 11.2.5</b>
Sub-contractors, <i>See</i> Contracted agencies	
Subpoenas	Section 11.3.7
Supervisors, <i>See also</i> Management, use of health information in	Section 6.3.1, <a href="#">Section 6.4</a>
<b>T</b>	
Telehealth records	<a href="#">Section 15.11</a>
Telephone transmittal of information	Section 9.2.4, <a href="#">Section 10</a>
Third parties	
Health service providers	Section 15.1
Information collected from	Section 7.4.1
Seeking access to information	<a href="#">Section 12.3.1.1</a>
Threats to health or welfare, <i>See</i> Health, preventing a serious and imminent threat	
Tissue donors, information about	<a href="#">Section 15.9.5</a>
Torres Strait Islander health information	Section 15.9.1
Training	
In electronic records	Section 16.3.2
Presentations, seminars and conferences	<a href="#">Section 9.2.6</a> , <a href="#">Section 11.2.5</a>
Responsibilities under privacy law	<a href="#">Section 9.2.6</a> , <a href="#">Section 11.2.5</a>
Use of records during	<a href="#">Section 9.2.6</a> , <a href="#">Section 11.2.5</a>
Transborder flows	Section 13.2
Transfer of records	Section 9.2.4, <b>Section 15.13.5</b>
Transfer of records outside NSW	Section 13.2
Treasury Managed Fund (TMF)	<a href="#">Section 14.3</a> , <a href="#">Section 15.6</a>
<b>U</b>	
Unlawful activity	<a href="#">Section 11.2.7</a> , <a href="#">Section 11.3.4</a>
Use of health records, <i>See also</i> Health records	Section 9, <b>Section 11</b> , <a href="#">Section 15</a> , <a href="#">Section 16</a>
<b>V</b>	
Verbal communications, <i>See also</i> Conversations	Section 7.4.4
Verbal consent	<b>Section 11.2.2.2</b> , <a href="#">Section 15.11</a>
Veterans' Affairs, Department of (Clth)	<a href="#">Section 11.3.14.2</a>
Violent behaviour	Section 11.2.3.2
Voice mail, not to be used for information	Section 9.2.4.1
<b>W</b>	
Website, NSW Health privacy	Section 6.6

Whiteboards, Patient journey boards	Section 9.2.9
Witness protection patients in custody	<a href="#">Section 8.3</a>
<a href="#">Work Health and Safety Act 2011</a>	Section 11.2.3.2, Section 11.3.12
Workcover, See also Insurance and compensation	Section 11.3.12

## Y

Young person	
Definition of	<a href="#">Section 1</a>
Protection of	<a href="#">Section 11.3.2</a>
Youth-friendly privacy resources	Section 7.4.7

---

NSW Health

[health.nsw.gov.au](https://health.nsw.gov.au)

