# Policy Directive

NSW HEALTH

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

## Privacy Manual (Version 2) - NSW Health

| | |
|---|---|
| **Document Number** | PD2005_593 |
| **Publication date** | 03-Jun-2005 |
| **Functional Sub group** | Corporate Administration - Governance<br>Corporate Administration - Information and data<br>Clinical/ Patient Services - Records<br>Personnel/Workforce - Conduct and ethics<br>Personnel/Workforce - Security |
| **Summary** | The NSW Health Privacy Manual provides operational guidance for health service staff to the legislative obligations imposed by the Health Records and Information Privacy Act 2002. The document outlines procedures to support compliance with the Act in any activity that involves personal health information. |
| **Replaces Doc. No.** | Privacy Manual (Version 1) 2004 - NSW Health [PD2005_362] |
| **Author Branch** | Legal and Legislative Services |
| **Branch contact** | Victoria Davison 9391 9092 |
| **Applies to** | Area Health Services/Chief Executive Governed Statutory Health Corporation, Board Governed Statutory Health Corporations, Affiliated Health Organisations - Non Declared, Affiliated Health Organisations - Declared, Community Health Centres, Dental Schools and Clinics, Government Medical Officers, NSW Ambulance Service, NSW Dept of Health, Public Health Units, Public Hospitals |
| **Audience** | ALL |
| **Distributed to** | Public Health System, Community Health Centres, Dental Schools and Clinics, Government Medical Officers, NSW Ambulance Service, NSW Department of Health, Public Health Units, Public Hospitals |
| **Review date** | 30-Jun-2011 |
| **Policy Manual** | Not applicable |
| **File No.** | 04/1924-01 |
| **Previous reference** | N/A |
| **Status** | Active |

**Director-General**

This Policy Directive may be varied, withdrawn or replaced at any time.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

NSW HEALTH

# NSW Health Privacy Manual

*Version 2*

**Policy Directive PD2005_593**

**NSW DEPARTMENT OF HEALTH**
73 Miller Street
NORTH SYDNEY NSW 2060
Tel. (02) 9391 9000
Fax. (02) 9391 9101
TTY. (02) 9391 9900
**www.health.nsw.gov.au**

This work is copyright. It may be reproduced in whole or in part for study 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 Department of Health.

© NSW Department of Health 2005

SHPN (PHCP) 050066
ISBN 0 7347 3813 7

For further copies of this document please contact:
Better Health Centre – Publications Warehouse
Locked Mail Bag 5003
Gladesville NSW 2111
Tel. (02) 9816 0452
Fax. (02) 9816 0492

Further copies of *Health Privacy Policy* documents can be downloaded from the:
NSW Health website: www.health.nsw.gov.au
Intranet: internal.health.nsw.gov.au/publications

June 2005

# Contents


**1 Definitions and acronyms .....1**

**2 Introduction .....3**

**3 Scope .....4**

3.1 Who is bound by the manual? .....4

3.2 What sort of information does the manual cover? .....4

3.3 What is not covered? .....4

3.4 What our patients have a right to expect .....5

3.5 What health staff and service providers have a right to expect .....5

3.6 Quick reference to structure of manual .....5

3.7 What other NSW Health resources should be considered .....6

3.8 Summary of the Health Privacy Principles (or HPPs) .....6

**4 Other obligations .....8**

4.1 Privacy laws and related legislation .....8

4.1.1 *Health Administration Act 1982* .....8

4.1.2 *Mental Health Act 1990* .....8

4.1.3 *Public Health Act 1991* .....8

4.1.4 *Commonwealth Privacy Act 1988* .....9

4.2 Other laws regulating information management .....9

4.2.1 *NSW State Records Act 1998* .....9

4.2.2 *NSW Freedom of Information Act 1989 (FOI)* .....9

4.3 Common law and professional obligations .....10

4.3.1 Duties of confidentiality .....10

4.3.2 Registered health professionals .....10

4.3.3 Health service codes of conduct .....10

**5 Key concepts .....11**

5.1 Personal health information .....11

5.2 Personal information .....11

5.3 De-identified information .....12

5.4 Consent .....12

5.4.1 Elements of consent .....12

5.4.2 Implied consent .....13

5.4.3 Express consent .....13

5.4.4 Deciding if consent is needed .....13

5.5 Test for capacity .....14

5.5.1 General rule .....14

5.5.2 Minors .....14

5.6 Authorised representative .....14

5.7 "Reasonable and practicable" .....15

**6 Responsibilities under privacy law .....17**

6.1 Chief Executives .....17

6.1.1 Key obligations .....17

6.1.2 Staff training .....17

6.2 Privacy Contact Officer .....17

6.3 Other staff .....16

6.3.1 Managers and supervisors .....16

6.3.2 Individual service providers .....16

6.3.3 Funding and grants administrators .....17

6.3.4 Information systems and information technology managers .....17

6.4 Contracted agencies .....17

6.5 Compliance tips .....17

**7 Collecting personal health information .....18**

7.1 When can you collect information? (HPP 1) .....18

7.2 How should information be collected? (HPP 2) .....18

7.3 Who should information be collected from? (HPP 3) .....19

7.4 Informing people about what is collected (HPP 4) .....19

7.4.1 Who do you need to inform if you have collected the information? .....19

7.4.1.1 The person to whom the information relates lacks capacity ....19
7.4.1.2 The person waives the right to be told ....19
7.4.1.3 Informing a person will prejudice their interests or pose a threat ....19
7.4.1.4 Where the information is collected from a third party ....20
7.4.2 What do they need to be told? ....20
7.4.3 When should they be told? ....20
7.4.4 How should they be told? ....20
7.4.5 Privacy leaflet for patients ....21

**8. Anonymity (HPP 13) ....22**

8.1 When may providing a service anonymously be impracticable? ....22
8.2 When may providing a service anonymously be unlawful? ....22

**9. Retention, security and protection (HPP 5) ....23**

9.1 Retention and disposal of personal health information ....23
9.2 Security of personal health information ....23
9.2.1 Paper records ....23
9.2.2 Computer systems and applications ....23
9.2.3 Safeguards when delivering and transmitting information ....24
9.2.3.1 Telephone ....24
9.2.3.2 Facsimile ....24
9.2.3.3 Mail ....24
9.2.3.4 Electronic discharge referrals/summaries ....24
9.2.3.5 Other electronic transmission, including email ....25
9.2.4 Printing and copying ....25
9.2.5 Training and demonstrations ....25
9.2.6 Conversations ....25
9.2.7 Visibility of screens ....25

**10 Accuracy (HPP 9) ....26**

**11 Using & disclosing personal health information (HPP 10 & 11) ....27**

11.1 Use and disclosure for the "primary purpose" ....27
11.2 Use and disclosure for a "secondary purpose" ....27
11.2.1 Directly related purpose ....28
11.2.1.1 "Directly related purpose" ....28
11.2.1.2 "Reasonable expectation" ....29
11.2.1.3 Outside client/patient's "reasonable expectation" ....29
11.2.2 Consent ....29
11.2.2.1 Where a third party seeks access ....30
11.2.2.2 Where the health service seeks to use or disclose ....30
11.2.3 To prevent a serious and imminent threat to health or welfare ....31
11.2.3.1 General guidelines ....31
11.2.3.2 Where staff may be at risk ....31
11.2.3.3 *Public Health Act* – Notification of public health risk for HIV ....32
11.2.4 Management, training or research ....32
11.2.4.1 When to use this exemption ....32
11.2.4.2 Statutory Guidelines ....33
11.2.5 Finding a missing person ....34
11.2.6 Investigating and reporting wrong conduct ....34
11.2.7 Law enforcement agencies, including police ....34
11.2.7.1 What is a "law enforcement agency?" ....34
11.2.7.2 What sort of information can be provided? ....34
11.2.7.3 How should requests from law enforcement agencies be handled ....35
11.2.8 Investigative agencies ....36
11.2.9 Disclosure on compassionate grounds ....36
11.3 Use and disclosure authorised by law (HPPs 10(2) and 11(2) ....37
11.3.1 NSW Department of Health officers and environmental health officers ....37
11.3.2 Department of Community Services (DoCS) ....37
11.3.3 Prison officers (access to health records of prisoners) ....37

11.3.4 Reporting "serious criminal offences".....37
11.3.5 Coroner.....38
11.3.6 Search warrants and subpoenas.....38
11.3.7 Health Care Complaints Commission.....39
11.3.7.1 Powers to enter premises.....39
11.3.7.2 Powers to obtain documents.....39
11.3.8 The Ombudsman.....39
11.3.9 Official visitors.....39
11.3.10 Child death review team.....39
11.3.11 Workcover.....39
11.3.12 Commonwealth agencies.....39
11.3.12.1 Family and community services.....39
11.3.12.2 Veterans' Affairs.....39
11.3.12.3 Immigration and Multicultural and Indigenous Affairs (DIMIA).....40
11.3.13 Statutory reporting requirements.....40
11.3.14 Information required by the Minister or Premier.....40

**12 Patient access and amendment (HPPs 6, 7 & 8).....41**

12.1 Access to personal health information (HPPs 6 & 7).....41
12.2 Interaction of *HRIP Act* and *FOI Act*.....41
12.3 Process for determining access.....41
12.4 Obtain proof of identity.....42
12.5 Conditions of access.....42
12.6 Fees and charges.....42
12.7 Additions and corrections.....42
12.7.1 Where an alteration is included.....42
12.7.2 Where an alteration is refused.....42

**13 Miscellaneous HPPs.....43**

13.1 Identifiers (HPP 12).....43
13.2 Transferring personal health information out of NSW (HPP14).....43
13.2.1 Within Australia.....43
13.2.2 Outside Australia.....43
13.3 EHR linkage at state or national level (HPP 15).....44

**14 Complaints handling.....45**

4.1 General principles.....45
4.2 Sanctions.....45

**15 Common privacy issues.....46**

15.1 Third party health service providers.....46
15.1.1 Informing patients.....46
15.1.2 Health service provider obligations.....46
15.1.3 Addressing patient concerns.....46
15.1.4 Conclusion of care.....46
15.1.5 Discharge referrals to GPs and others.....46
15.1.6 Records of a patient's family members.....47
15.2 Requests from State and Federal Police.....47
15.2.1 Where disclosure to police is authorised by patient.....47
15.2.2 Where access is not authorised by patient.....47
15.2.3 Search warrants.....47
15.2.4 Police interviews.....47
15.2.4.1 Interviews with clients/patients.....47
15.2.4.2 Interviews with clients/patients under the age of 16.....47
15.2.4.3 Interviews with victims of sexual assault.....47
15.2.4.4 Interviews with staff.....47
15.3 Child protection issues.....47
15.3.1 Reporting children at risk (Section 27).....48
15.3.2 Information sharing with DoCS (Section 248).....48
15.3.3 Medical examinations (Section 173).....48
15.3.4 Restrictions on access to child protection records.....48
15.3.4.1 General rules.....48
15.3.4.2 Requests for information by parents.....48
15.3.4.3 Staff safety.....48
15.4 Health examinations of school children.....49
15.5 Use of interpreters.....49
15.6 Legal claims and insurance.....49
15.6.1 Claims manager and treasury managed fund.....49
15.6.2 Client/patient's legal representative.....49
15.6.3 Client/patient's insurer.....49

15.7 Media and other enquiries about hospital patients ....50
15.7.1 Enquiries about clients/patients ....50
15.7.2 Other safeguards for enquiries sections ....50
15.7.3 Media queries ....50
15.7.3.1 Responsibility for media liaison ....50
15.7.3.2 Accident victims ....50
15.7.3.3 Information about medical practitioners ....50
15.7.3.4 Tapes or images of clients/patients ....50
15.8 Fundraising ....50
15.8 1 Limits on what information may be used ....51
15.8.2 Use of mailing lists ....51
15.8.3 Organisations with a commercial interest ....51
15.9 Information specific laws and policies ....51
15.9.1 Aboriginal health information ....51
15.9.2 Adoption information ....52
15.9.3 Service based policies ....52
15.9.3.1 Genetics services ....52
15.9.3.2 Child protection services ....52
15.9.3.3 Sexual assault services ....52
15.9.4 Service based practices ....53
15.9.4.1 Drug and alcohol services ....53
15.9.4.2 Sexual health services ....53
15.9.5 Organ and tissue donor information ....53
15.9.6 Managing public health risks ....54
Reporting of certain medical conditions and diseases ....54
Contact tracing ....54
Undertaking public health inquiries ....54
15.10 Deceased patients ....54
15.11 Telehealth ....55
15.12 Community health records ....55
15.12.1 Group houses/hostels ....55
15.12.2 Group sessions ....55
15.12.3 Family consultations ....55
15.13 Maintaining the health record ....55
15.13.1 Quality of health records ....55
15.13.2 Accuracy and completeness ....56
15.13.3 Control of health records ....56
15.13.4 Removal ....56
15.13.5 Transfer ....56
15.13.6 Storage, archiving and disposal ....56
15.13.7 Health facility closures ....57
15.14 NSW data collections ....57
15.14.1 NSW Health data ....57
15.14.2 Health Information Resources Directory (HIRD) ....57
15.14.3 Staff roles ....57
15.14.4 Access to data collections ....58
15.14.4.1 Conditions of access ....58
15.14.4.2 Records linkage ....58
15.14.4.3 NSW Department of Health Ethics Committee (DOHEC) ....58

**16 Electronic health records ....59**
16.1 Fundamental principles ....59
16.2 *Evidence Act* ....59
16.3 Accountability ....60
16.4 Access and quality control ....60
16.5 Patient access ....60

**Appendix 1: List of relevant policies ....61**
A.1.1 NSW policy directives ....61
A.1.2 Other NSW health policies ....61
A.1.3 Other government policies ....61

**Appendix 2: List of relevant laws ....62**

**Appendix 3: Pro forma privacy undertaking ....63**
A.3.1 Privacy undertaking (general) ....63
A.3.2 Electronic medical record privacy undertaking ....64
A.3.3 Contractual provisions ....65

**Appendix 4: Pro forma privacy notices ....66**
A.4.1 For fax cover sheet ....66
A.4.2 For patient charts/end of patient bed ....66
A.4.3 For health records ....66

**Appendix 5: Pro forma privacy leaflet for patients ....67**

# Definitions and acronyms 1

Frequently used terms are defined as follows in the context of this document.

**Affiliated health organisation** – An organisation or institution listed in Schedule 3 of the *Health Services Act 1997.*

**Area health service** – An area health service constituted under the *Health Services Act*.

**Capacity** – see 5.4.

**Chief Executive** – Under the *Health Services Act*, the Chief Executive of an area health service or a statutory health corporation or the person responsible to the governing body of an affiliated health organisation for management of its recognised establishments and services.

**Client/patient** – Any person to whom a health service provider owes a duty of care in respect of provision of health services.

**Confidentiality** – see 4.3.1.

**Consent** – see 5.3.

**Data** – A representation of facts, concepts or instructions in a formalised manner suitable for communication, interpretation or processing by human beings or by automatic means.

**Department of Health** – The NSW Department of Health as established under Section 6 of the *Health Administration Act 1982*.

**Disclosure of personal health information** – Refers to the communication or transfer of information outside a health service, through giving a copy of the information to another organisation or individual, allowing another organisation or individual to have access to the information or giving out summaries, or communicating the information in any other way.

**DoCS** – Department of Community Services.

**DOHEC** – The NSW Department of Health Ethics Committee, a Human Research Ethics Committee, established in accordance with NH&MRC Guidelines.

**FOI** – *Freedom of Information Act 1989*.

**Health service** – A public health organisation (including an area health service) or the Ambulance Service of New South Wales.

**Health service provider** – A health care provider, health information manager, clerical, administrative, technical or scientific worker, volunteer, student, consultant or other person working in the public health system.

**Health record** – A documented account, whether in hard or electronic form, of a client's/patient's health, illness and treatment during each visit or stay at a health service (and includes a medical record).

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

**Hospital** – Under the *Health Services Act*, an institution at which relief is given to sick or injured people through the provision of care or treatment.

**HPPs** – The Health Privacy Principles established under the *Health Records* and *Information Privacy Act 2002*. There are 15 HPPs.

**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.*

**Immediate family member** – Defined under Section 4 of the *HRIP Act* to be a person who is:

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

**Medical practitioner** – A person registered to practice medicine under the *Medical Practice Act 1992*.

**Medical record** – see health record.

**NHMRC** – National Health & Medical Research Council.

**NSW Health** – Comprises the NSW Minister for Health, the Minister Assisting the NSW Minister for Health, the NSW Department of Health, Public health organisations.

**Parental responsibility** – Defined in Section 8 of the *HRIP Act* to be all the duties, powers, responsibility and authority which, by law, parents have in relation to their children.

**PCO** – Privacy Contact Officer, see 6.2.

**Personal health information** – see definition in 5.1.

**Personal information** – see definition in 5.2.

***PPIP Act*** – *The Privacy and Personal Information Protection Act 1998.*

**Potentially identifiable data** – Records from which names and addresses have been removed but from which it might still be possible to identify an individual indirectly by using remaining data such as an identity number or some combination of other, not directly identifying data items.

**Power of attorney** – A formal document in which a person authorizes a second person to act on their behalf. It can be general, or limited to certain decisions. An enduring power of attorney is a special type of power of attorney which allows decisions to be made where the person loses mental capacity.

**Public health organisation** – Under the *Health Services Act*, an area health service or a statutory health corporation, or an affiliated health organisation in respect of its recognised establishments and services.

**Public health system** – Under the *Health Services Act*, a public health system consists of all area health services, statutory health corporations and affiliated health organisations in respect of their recognised establishments and services.

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

**Security** – A tangible set of physical and logical mechanisms which can be used to protect information held in hard copy, computer systems and information and telecommunications infrastructure.

**Senior health care provider** – The Medical Superintendent, Director of Clinical Services or other supervising senior health care provider, if appropriate.

**Statutory guidelines** – Refers to guidelines issued by the NSW Privacy Commissioner.

**Statutory health corporation** – A corporation, listed in Schedule 2 of the *Health Services Act*, which provides certain health and health support services other than on an area basis (including The Royal Alexandra Hospital for Children and Justice Health).

**Treating health care provider** – A medical practitioner or other health care provider who is responsible for care to the client/patient at the time access to personal health information occurs.

**Use of personal health information** – Refers to the communication or handling of information within a health service. 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.

# Introduction

# 2

This is the second edition of the NSW Health Privacy Manual. The first edition was released in July 2004, in conjunction with the *Health Records and Information Privacy Act 2002*. A six-month consultation period followed in conjunction with training on the *Act*. During this time, the Department received a substantial number of submissions from both health service providers and consumers. While the submissions were generally supportive of the content of the manual, they also made suggestions for clarification and additions to various parts of the document. These comments and suggestions for improvement have been taken into account in producing the second edition. The manual has been developed with the assistance of the NSW Health Privacy Reference Group.

As noted in the first edition, privacy in Australia has moved from a policy based system to one regulated by law. In NSW, these laws are the *Health Records and Information Privacy Act 2002* (*HRIP Act*) which regulates health privacy, and the *Privacy and Personal Information Protection Act 1998 (PPIP Act)* which remains applicable to non-health information. As privacy policy is set by legislation, the role of this manual is to provide operational guidance to assist in compliance with the *HRIP Act*.

The manual provides a guide to the legislative obligations imposed on the health system by the *HRIP Act* and outlines procedures to support compliance with the *Act* in any activity that involves personal health information. Specific purposes include:

- to ensure personal health information is collected, stored and used in accordance with the *HRIP Act*
- to provide health service personnel with assistance and practical tips for complying with the *HRIP Act*
- to acknowledge and delineate the responsibility of the NSW public health system to ensure that the privacy of client/patient information is protected
- to meet the need of health workers for clear guidance on what is acceptable and what is not when dealing with personal health information in order to remove pressure and uncertainty from those who are involved in the day to day administration of such information
- to constitute a benchmark which can be used for auditing performance.

The Health Privacy Principles (or HPPs) contained in the *HRIP Act* establish 15 rules for the management of information. Some of these rules will mainly be relevant when setting up data collections or patient information systems, such as:

- Collection Principles (HPPs 1–3).
- Retention and Security (HPP 5).
- Identifiers (HPP 12).
- Linkage of Electronic Records (HPP 15).

Other HPPs will be relevant to how you interact with clients and patients and meet their information needs:

- Collection Principle (HPP 4).
- Access (HPPs 6–7).
- Amendment (HPP 8).
- Anonymity (HPP 13).

Others will also be important in the day to day use of personal health information in the NSW public health system, and deciding when and how to share that information:

- Accuracy (HPP 9).
- Use (HPP 10).
- Disclosure (HPP 11).
- Transfer of Information Across State Borders (HPP 14).

While the HPPs are applicable across the board, they will be particularly relevant if involved in the above activities. In these cases, you should look particularly closely at the issues raised in the manual.

The manual will be kept under ongoing review to ensure its contents remain useful, relevant and up-to-date. If you have any feedback on the manual, it should be sent to:

**Legal and Legislative Services**
NSW Department of Health
LMB 961 NORTH SYDNEY 2059
E-mail: privacy@doh.health.nsw.gov.au

# 3 Scope

## 3.1 Who is bound by the manual?

The manual applies to all people who work within the NSW public health system, including employees, contractors and other health service providers who, in the course of their work, have access to personal health information. These include:

- providers of health services such as doctors, nurses, case managers, visiting providers and allied health staff
- administrators, clerical and service staff
- technical, scientific and laboratory personnel
- auditors
- interpreters
- volunteers
- students
- consultants
- temporary and contract staff
- external custodians of information owned by the Department.

The manual applies to NSW health services, those being:

- NSW Department of Health
- Ambulance Service of New South Wales
- area health services
- affiliated health organisations
- statutory health corporations
- any other health service provided by the public health system including nursing homes, hostels and group homes, community health services, drug and alcohol services, allied health programs, dental and early childhood services, multi-purpose services, scientific and laboratory services and health promotion and public health services
- non-government organisations receiving funding from the Department where compliance is included in the terms of their Funding Agreement
- private hospitals and day procedure centres treating public patients on a contractual basis (limited to records of public patients)
- staff of Health Professional Registration Boards employed by the Health Administration Corporation (excluding Medical, Dental and Pharmacy Boards).

The policy and procedures apply to people whose employment is part time, temporary, contractual, casual or short-term. These include volunteers and people who do unpaid work either as community volunteers, or clinicians working or observing as research fellows etc.

## 3.2 What sort of information does the manual cover?

The manual covers personal health information as defined in the *HRIP Act* 2002 being personal information that is identifying information collected from or about individual people in order to provide them with health services.

Both the *HRIP Act* and the manual cover all types of dealings with personal health information, including collection, storage, security, use, disclosure, access, transfer and linkage of records. They apply to personal health information in any format, including electronic and online formats as well as paper based records. While different formats will require different approaches and procedures, the underlying principles remain the same.

## 3.3 What is not covered?

The *HRIP Act* and the manual do NOT apply to:

- information that is not "personal information" but which may be considered sensitive such as tender documents, private hospital registration information or Cabinet documents
- information that is not personal information as it is "de-identified" or because the identity of a person is not reasonably ascertainable from the information
- personal information which is not health information, such as payroll records or personnel files (these are regulated by the *PPIP Act*)
- statistical or other aggregated information.

### 🕮 Further guidance

On managing information not covered by the *HRIP Act*:

- PD2005_554: Privacy Management Plan.
- PD2005_130: Principles and Minimum Standards for the Development of Health Services Codes of Conduct.
- NSW Public Service Personnel Handbook.
- NSW Health Purchasing and Supply Manual.

## 3.4 What our patients have a right to expect

Clients/patients should be informed that:

- their personal health information will be protected in accordance with the *HRIP Act*
- their personal health information will be given to another person only if this is important for their health care or can be otherwise legally and ethically justified
- they are, subject to limited exceptions, entitled to access their own Health Records and have those records amended to correct inaccuracies
- provided it is both legal and practicable to do so, they will have the opportunity to obtain services anonymously
- comprehensive clinical information will be available to their health care providers to enable optimal care.

### 🕮 Further guidance:

- Section 7: Collecting personal health information.

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

NSW Health is committed to ensuring that information which supports the provision of health care is readily available to authorised users, when and where it is needed and is delivered in a timely and efficient manner. Accordingly the manual supports the principles in the *HRIP Act* which also promote:

- the integrity of data, so that information is accurate, complete and up-to-date; information integrity is critical for quality client/patient care; evaluation of services, medical research and the maintenance of public health
- authorised persons who need information for legitimate health purposes have ready access to it; recognising that if clinical information is not readily available to providers of health services, the care or interests of clients/patients may be compromised
- the optimum use of data, primarily for the benefit of those clients/patients to whom the data relates but also for the general betterment of the health of the population of New South Wales through public health surveillance and medical research.

## 3.6 What other NSW Health resources should be considered

This manual provides a broad overview of the key privacy obligations established under the *HRIP Act*. There are however a range of other NSW Health policies which are also relevant to the collection, use storage and disclosure of information in NSW Health.

The main policies are referenced in the body of the manual. In addition, a comprehensive list of related NSW Health policies is set out in Appendix 1. The manual should be read in conjunction with these policies.

## 3.7 Quick reference to structure of manual

| | |
|---|---|
| For a general overview of the rationale and purposes for this manual | **Go to Section 2.1** |
| For a summary of the Heath Privacy Principles (HPPs) under the *HRIP Act* | **Go to Section 3.8** |
| 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 the HPPs | **Go to Section 5** |
| For a detailed explanation of the HPPs | **Go to Sections 7–13** |
| If you have received a complaint, or need to conduct an internal review | **Go to Section 14** |
| If you need to check how to deal with common privacy issues arising in Health | **Go to Section 15** |
| **For:** | |
| – list of relevant NSW Health policies | **Go to Appendix 1** |
| – list of relevant laws | **Go to Appendix 2** |
| – pro forma privacy undertaking | **Go to Appendix 3** |
| – pro forma privacy notices | **Go to Appendix 4** |
| – pro forma patient leaflet | **Go to Appendix 5** |

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

| **Collection principles** |
|---|
| **HPP 1 Purposes of collection of personal health information**<br>Personal health information must be collected by lawful means and for a lawful purpose. The purpose must be directly related to, and reasonably necessary for, an organisation's functions or activities. |
| **HPP 2 Collection and information sought must be relevant, not excessive, accurate and not intrusive** |
| **HPP 3 Collection from individual concerned**<br>Personal health information must be collected from the individual it relates to, unless that is unreasonable or impractical. |
| **HPP 4 Individual to be made aware of certain matters**<br>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.<br>The individual should be told what agency is collecting the information and that they have a right to access it. This information should generally also be given to the individual where information about them is collected from someone else, unless certain exemptions, listed in the *Act* and the Guidelines apply. |
| **Security principles** |
| **HPP 5 Retention and security**<br>Personal health information held by public health agencies must be securely housed and protected against loss or misuse. Information must be kept only as long as is necessary for the purpose (or as required by a law, such as the *NSW State Records Act 1998*), and must be disposed of securely. |
| **Access and amendment principles** |
| **HPP 6 Information about personal health information held by organisations**<br>Organisations that hold personal health information must allow individuals to find out if they hold information about that individual, and, if so, what kind of information they hold, what it is used for, and whether and how the individual can access it. |

**HPP 7 Access to personal health information**

Individuals must be allowed to access the personal health information held about them. This must be done without excessive delay or expense.

**HPP 8 Amendment of personal health information**

Individuals may request that their personal health information be amended to ensure that it is accurate, relevant, up-to-date, complete and not misleading.

Organisations must either make the requested amendments or, if requested, attach to the information a statement by the individual of the amendment they sought.

**Accuracy principles**

**HPP 9 Accuracy**

Organisations must take reasonable steps to ensure that the personal health information they hold is relevant, up-to-date, complete and not misleading.

**Use principles**

**HPP 10 Limits on use of personal health information**

Personal health information can be used for the purpose for which it was collected, or for other purposes recognised by the *Act*. These include "secondary purposes" 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 and imminent threats to individuals or the public.

**Disclosure principles**

**HPP 11 Limits on disclosure of personal health information**

The provisions for disclosure of personal health information are the same as those for use of this information.

They also include a provision that a person's personal health information may be disclosed to immediate family members for compassionate reasons, provided that this is not contrary to the expressed wish of the individual.

**Other principles**

**HPP 12 Identifiers**

Identifiers can only be applied to personal health information if this is reasonably necessary to carry out the organisation's functions.Public health system identifiers may be used by private sector agencies, but only in defined circumstances and with strict controls.

**HPP 13 Anonymity**

Provided that it is lawful and practicable, individuals should be given the option of not identifying themselves when dealing with health organisations,.

**HPP 14 Transborder data flows and data flows to Commonwealth agencies**

As a general principle, personal health information must not be transferred to a Commonwealth agency or an organisation in another state jurisdiction unless the receiving agency applies personal health information privacy policies and procedures substantially similar to those of NSW.

**HPP 15 Linkage of health records**

Personal health information must not be included in a system that links health records of one health service with health records in another health service unless the individual it relates to has expressly consented.

# 4 Other obligations

## 4.1 Privacy laws and related legislation

Privacy obligations in NSW arise from two separate laws. First, the *Privacy and Personal Information Protection Act 1998*, which regulates personal information in the public sector, and second, *Health Records and Information Privacy Act 2002*, which regulates personal health information.

There are however other pieces of legislation which impose specific controls on when and how information can be used and disclosed in the health system. The most important of these are:

### 4.1.1 *Health Administration Act 1982*

The *Health Administration Act* covers any information which is provided or recorded pursuant to any *Act* in the health portfolio. It is binding on all persons working in the NSW health system. Under Section 22 of the *Act* information cannot be disclosed unless certain specified criteria are satisfied. These criteria cover:

- where the person to whom the information relates consents to the release
- where the release occurs in connection with the administration of health legislation (ie where other legislation such as the *Public Health Act* authorises or requires disclosure)
- where the release is for the purposes of legal proceedings arising out of health legislation, eg pursuant to a court order or subpoena
- when there is an 'other lawful excuse' such as, orders under other court proceedings, assisting the police in investigating a specific criminal offence, or a lawful direction by the Minister or Director-General
- in circumstances set out in Regulations under the *Act*.

Regulations currently exist to allow the Chief Health Officer to release epidemiological data and the Director-General of the NSW Department of Health to release other information for the purposes of research. Such data are only released to bona fide researchers and on condition that the confidentiality of data is maintained. Clause 13 of the Health Administration General Regulation, allows these disclosures if:

- the information is epidemiological data
- the disclosure is made in accordance with the written approval of the Chief Health Officer
- that approval describes the information that is authorised to be disclosed and names the person or body to whom disclosure is authorised.

The *Act* provides for a penalty of a fine of up to $1,000 or imprisonment for a term not exceeding six-months.

### 4.1.2 *Mental Health Act 1990*

Section 289 of the *Mental Health Act* prevents release of information collected under the *Act* unless certain criteria, similar to those set out above in 4.1.1, are met. It is of particular relevance to people working in the mental health field. The *Act* provides for a penalty of a fine of up to $5,000 for unauthorised disclosure of information.

As at June 2005, the *Mental Health Act* was in the process of being revised. One of the main areas of reform identified as part of the review was the need to ensure the information sharing provisions under the *Act* properly meet carer and client/patient needs. For information on the status of these changes see www.health.nsw.gov.au/csd/llsb.

### 4.1.3 *Public Health Act 1991*

Section 75 of the *Public Health Act* prevents release of information collected under the *Act* unless certain criteria, similar to those set out above in 4.1.1, are met. Clause 81a of the Public Health Regulation allows the release of epidemiological data where there is written approval from the Chief Health Officer.

The most important confidentiality provision in the *Public Health Act* is Section 17 which deals specifically with "HIV/AIDS related information". Under the *Act* this means two things the fact that a person:

- has had or is going to have a HIV test
- is HIV positive.

Section 17 places strict limitations on the release of this information, which can only be disclosed:

- to a person involved in the care or treatment or counselling of the person to whom the information relates, if the information is required in connection with that care
- with the consent of the person to whom the information relates
- in connection with the administration of an *Act*
- under an order of a court or a person authorised to examine witnesses.

The *Act* provides for a penalty of a fine of up to $5,000 for unauthorised disclosure.

### 4.1.4 *Commonwealth Privacy Act 1988*

This *Act*, does NOT apply to the NSW public sector. The *Act* is limited to the regulation of the Commonwealth public sector and, following amendments which commenced in December 2001, it regulates the private sector in NSW including non-government organisations. Its provisions relating to health information do not therefore apply to NSW Health and should not be relied on.

NSW Health agencies however should be aware that the *Commonwealth Privacy Act* does bind non-government organisations and private sector health providers (such as individual medical practitioners and private hospitals), and so may be relevant to the way these organisations interact with NSW Health.

## 4.2 Other laws regulating information management

### 4.2.1 *State Records Act 1998*

The *State Records Act* provides for the retention and disposal of records held by public sector agencies. The *Act* is not affected by the *HRIP Act*.

### 4.2.2 *Freedom of Information Act 1989* (FOI)

The *FOI Act* allows any person to apply for access to any information held by government. It is different from the *HRIP Act* as it is designed to facilitate open and transparent Government and is not restricted to personal information, whereas privacy laws are designed to provide individuals with greater knowledge and control over their own information.

In the past, FOI has been used by patients as an efficient and relatively cheap means for obtaining access to their own health records.

As a general principle health services should rely on the access provisions in privacy law, rather than FOI. FOI may however still be used where:

The client/patient (including their legal representative) requests access under FOI. Their application should be processed, and should not be refused simply because they could use the *HRIP Act*.

The information sought relates to a number of people or is sought in the context of a family dispute or raises other contentious issues. FOI provides a structured process for consultation with people who may be affected by release of information. It may therefore be a useful alternative in such cases.

Where a family seeks information about a relative who is deceased, and there is no appropriate "authorised representative" to consent to the disclosure.

### 🕮 Further guidance:

- **Section 12:** Access and amendment.

## 4.3 Common law and professional obligations

### 4.3.1 Duties of confidentiality

Health service providers owe patients a common law duty of confidentiality in relation to information obtained as part of the treating relationship. The duty is based in part on contract law and also on the "fiduciary duty" of an individual practitioner to his or her patients. The duty is not absolute and there are circumstances where a provider may lawfully disclose the information. These situations include where the client/patient waives their right to confidentiality, or where there is some statutory or other lawful excuse – such as for example, a court order or subpoena, or statutory provisions for mandatory notification (as occurs in relation to suspected child abuse, and certain notifiable diseases). Health service providers should consider their common law duties when considering release of information.

The common law also allows a disclosure to be made "in the public interest". This recognises that there will be circumstances where the public benefit of the information being disclosed is sufficient to outweigh the public interest in maintaining confidentiality. The exact nature and extent of this interest, and when it will apply however, remains somewhat uncertain, but generally tends to reflect similar types of circumstances to those recognised in privacy law.

### 4.3.2 Registered health professionals

Some health professional groups are registered under statute. This health professional registration legislation provides a basis for clinical and professional standards based on definitions of 'unsatisfactory professional conduct' and 'professional misconduct'. Breach of the confidence owed by a health service provider to a client/patient may constitutes 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. More broadly, they are a reflection of the prevailing view of proper conduct among the health professions.

### 4.3.3 Health service codes of conduct

The principles and minimum standards for the development of health service codes of conduct have been issued by the Department to provide a framework for the development of local codes of conduct by health services. In line with Premier's Department requirements, codes of conduct aim to provide guidance for staff in relation to decisions, actions and general conduct in their employment. They promote 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.

# Key concepts

# 5

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 Personal health information

Personal health information is personal information or an opinion about:

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

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

The *HRIP Act* also specifically includes genetic information about an individual that predicts or could predict the health of the individual or of their siblings, relatives or descendants.

The *HRIP Act* uses the term 'health information' to mean health information that identifies or could potentially identify an individual. This manual has however adopted the term "personal health information", to emphasise that neither the *HRIP Act* nor the manual regulates the collection, use or disclosure of other health-related information which is not about individuals, such as de-identified and epidemiological information. The requirements of the manual do not need to be followed in relation to this type of information.

## 5.2 Personal information

Personal information is defined in Section 6 of the *PPIP Act* as:

> *"any information or an opinion about a person whose identity is apparent or can reasonably be ascertained from the information or opinion"*

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

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

> **Example**: States and Territories are asked to participate in 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 and demographic information. Given the information is neither identifying or 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, 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.

The definition of personal information is much broader than that of personal health information, and is regulated by the *PPIP Act*. The legislative requirements for managing general personal information are different from the requirements for managing personal health information, and are not covered by this manual.

The obligations under privacy legislation apply to anyone who "holds" information. A health service holds personal health information if the information is in it's 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'. The most common ones are:

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

The obligations imposed by privacy law in relation to the collection of information (see Section 7) do not apply to unsolicited information.

Unsolicited information includes information which has been received by the health service provider in circumstances where the provider has not requested or does not need the information. For example, if an individual contacts a health service provider and discloses information which is not related to health services received or to be received.

### 🕮 Further guidance:

- PD2005_554: NSW Health Privacy Management Plan.

## 5.3 De-identified information

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

For information to be classified as de-identified it must not contain identifiers which, if linked with other information, could lead to the identity of a person. If there is a reasonable chance that the information is potentially identifiable, it cannot be classified as de-identified. Clearly, whether information can be considered de-identified will be dependant on the specific circumstances which arise in any disclosure.

**Example**: An MRN number, when used within the health service which created it, is likely to be "identifiable" but may be de-identified if released outside the health service, if the person receiving the MRN is unlikely to be able to link it with the personal identifying details of the client/patient.

**Example**: Data on small or unique groups, particularly in rural areas, may not be de-identified even where identifiers have been stripped.

De-identified information is exempt from privacy law and from the requirements of this manual. The Health Privacy Principles do not apply to de-identified information.

## 5.4 Consent

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

### 5.4.1 Elements of consent

- A consent should be **informed**. That is, there must be reasonable efforts to ensure that the person concerned has the information they need to understand what they are consenting to, why it is necessary or desirable, and what may be the results both of consenting and of not consenting.

- In order to be informed, the consent should also be **reasonably specific**. Reliance on general or blanket consents can be problematic if the client/patient later indicates they were not informed of the particular usage proposed.
- A consent should be **freely given**. That is, the person must not be coerced, pressured or intimidated. They should not feel they have no choice or that they do not have enough time to make up their mind.
- A consent should only be sought from a person who has **capacity** to consent (see 5.5).
- A consent should be **timely**. The validity of the consent is dependent on the client/patient's expectation. For example, if it is a standard consent for all clients/patients, the validity may be 12-months or longer if the client/patient is accessing ongoing services. However, if the consent is for a specific use and disclosure of information, the recommended timeframe is 3-months. The validity of a consent is more likely to be questioned where a lengthy period of time has passed or the client/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**, but when obtained should always be recorded, for example, by a notation in the client/patient's file.

### 5.4.2 Implied consent

Implied consent generally means that a person has not explicitly, either verbally or in writing given their agreement, but through their conduct or behaviour have "implied" consent, or by consenting to one action, they have impliedly consented to a range of other activities. The application of implied consent is limited. It will generally only arise in situation 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.

**Example**: A prisoner contacts the Justice Health Information Help Line to make a complaint regarding the health services provided to him whilst in prison, requesting that some action be taken to improve services available to him. By contacting the Help Line and requesting that some action be taken, the prisoner/patient is giving implied consent for the Help Line to contact Justice Health and access any personal health information about him which is necessary to deal with the complaint. In addition the Help Line should inform the prisoner/patient that it will be necessary to access his personal health information in order to respond to his request.

### 📖 Further guidance:

- PD2005_406: Patient Information and Consent to Medical Treatment.

### 5.4.3 Express consent

Express consent generally requires documentation of a consent which shows specific and clear intention on the part of the client/patient. A formal written consent will meet this requirement, provided the activity being consented to is clear on the face of the consent. There are two circumstances where the *HRIP Act* requires "express consent" from the client/patient. These are:

- under HPP 4, where a person can agree not to be given information about why their personal health information has been collected (see 7.4.1.2)
- under HPP 15, where a person consents to participate in a state or national EHR system (see 13.3).

### 5.4.4 Deciding if consent is needed

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

- using or disclosing the information for the **primary purpose** for which it was collected (see 11.1)
- using or disclosing the information for a **directly related secondary purpose**, and the client/patient would **reasonably expect** that use or disclosure. Reliance on a "directly related purpose" depends on what the client/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 11.2)

- **lawfully authorised** or required to use or disclose the personal health information (See 11.3).

Some common examples of when client/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 client/patient's GP where the client/patient (or their authorised representative) has provided the GP's details
- for current and future ongoing care and treatment purposes where the client/patient has been made generally aware that their information may be used in this way
- in emergency situations.

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

## 5.5 Test for capacity

### 5.5.1 General rule

A person cannot give consent, or make other decisions under privacy law if they do not have the necessary capacity to do so. Incapacity can be due to youth, 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.

*HRIP Act* establishes a test for capacity which states a person is incapable of giving consent if they:

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

The test does not therefore impose arbitrary rules dictating capacity on the basis of mental illness, disability or age. It requires a professional assessment of the individual's ability to make a specific decision. The complexity, seriousness and long term impact of any decision will impact on the level of understanding required in any particular case.

### 5.5.2 Minors

When treating a minor, the treating health care provider should assess the maturity of the client/patient, in particular their ability to understand the consequences of their decision. The following principles can be used as an age guide:

- Where a client/patient is less than 14-years of age, consent should generally be given by the parent or legal guardian.
- Where the client/patient is between 14 and 16-years of age, efforts should be made to obtain the consent of the parent or legal guardian unless the client/patient indicates a strong objection.
- Where the client/patient is 16-years of age or over, they should generally be capable of deciding on the access issue for themselves.

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

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

## 5.6 Authorised representative

The *HRIP Act* sets out the list of people who can be an authorised representative. They are:

- someone who has an enduring power of attorney for the individual
- a guardian as defined in the *Guardianship Act 1987*
- 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"
- any other person who is authorised by law to act for or represent the person (including an executor or administrator of a deceased estate)
- a "person responsible" under Section 33A of the *Guardianship Act*.

Who is a "person responsible" is determined via a hierarchy set out by the *Guardianship Act*, 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 client/patient with authority to make decisions regarding medical care
- if there is no enduring guardian, a spouse (including a de facto spouse) with whom the person has a close continuing relationship is the person responsible
- if there is no guardian or spouse, a person who has the care of the client/patient unable to consent is the person responsible. Such a person is regarded to have the care of the client/patient if they have provided, or have arranged to be provided, domestic services and support otherwise than for remuneration. Where the client/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 client/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 or friend may act as the person responsible provided they are not receiving remuneration for any services provided
- if the person is in the care of the Director-General under Section 13 of the *Guardianship Act*, the Director-General is the person responsible.

**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. 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.

**'Next of kin'** is a term widely used across the health system to allow a client/patient to nominate their partner or a relative as a person to contact. Typically, the name, contact details, date of birth and relationship to the client/patient of the 'next of kin' are collected and recorded by health facilities

The *HRIP Act* does not give a "next of kin" any authority to make decisions on behalf of the client/patient. Where a person is listed as a "next of kin", the health service provider should check whether they are an authorised representative before relying on that person to make a decision on behalf of the client/patient.

## 5.7 "Reasonable and practicable"

*HRIP Act* often qualifies requirements by reference to what is reasonable or practicable. These are concepts that cannot be readily defined as they will vary depending on the circumstances arising. There are however certain matters which can be considered in any case in deciding if something is "reasonable" or "practicable".

- consider what **most lay people** (not a health professional) may expect, or think acceptable, in this situation
- take into account the **context**, and all the surrounding circumstances. Will the activity have a major impact on the client/patient or others? Is a person's physical safety at risk? Is the issue urgent?
- assess the **cost and time** involved in complying, and whether they are appropriate having regard to the benefits or risks
- in assuming that an action is **reasonably necessary**, consider whether there are other ways of achieving the desired result
- do not assume that something is not reasonable or practicable simply because it is **inconvenient or a nuisance** (this is not an acceptable justification).

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

It is essential that health service providers be made aware of their individual rights and responsibilities in respect of safeguarding information privacy. They need to be informed about client/patients' rights of privacy and access to their own information. The importance of basic observances such as not discussing clients/patients publicly in a manner that would allow identification of individuals or groups, and keeping passwords secure cannot be over-emphasised.

# 6 Responsibilities under privacy law

## 6.1 Chief executives

### 6.1.1 Key obligations

- ensure that all employees are familiar with this manual
- ensure all employees have access to appropriate training
- ensure that all employees have access to appropriate material about their privacy obligations, including the NSW Health Privacy Manual in hard copy or via the intranet.

Designate a specific officer for the health service to whom all requests for guidance on information privacy may be referred and who should ensure, as far as possible, that policies and procedures are observed.

### 6.1.2 Staff training

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

All staff must have access to training in privacy principles and requirements. It is the responsibility of public health organizations to undertake such training. A privacy training kit is available to assist this process. It is the responsibility of staff to participate in such training.

## 6.2 Privacy Contact Officer

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

The principle tasks for privacy contact officers are:

- act as a first point of contact for members of the public for matters related to privacy
- serve as a focal point for health service staff for matters related to privacy
- act as a first point of contact with the NSW Department of Health and Privacy NSW for matters related to privacy.

A Privacy Contact Officer may also be involved with other tasks, such as:

- ensuring privacy complaints and requests for internal review are dealt with in accordance with PD2005_554: Privacy Management Plan
- disseminating information on privacy matters within the health service
- overseeing privacy training and education for health service staff.

## 6.3 Other staff

### 6.3.1 Managers and supervisors

Should provide leadership and direction to ensure that this 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 implement privacy law.

Should include privacy provisions in policies, procedures and service or project plans wherever appropriate.

### 6.3.2 Individual service providers

- should implement and comply with the *HRIP Act* and this manual
- should take responsibility for complying with the *HRIP Act* and this manual and for keeping up-to-date with any changes
- should report potential or actual breaches, risks, or other issues that may occur in relation to personal health information.

### 6.3.3 Funding and grants administrators

- should ensure funding processes, conditions and reporting requirements comply with privacy law
- should monitor the protection of personal health information in programs and initiatives funded by the public health system and initiate appropriate action to address any risks or shortcomings.

### 6.3.4 Information systems and information technology managers

- should ensure that the development and modification of information technology systems comply with privacy law
- should ensure that all documentation and processes for IT policy, procedures and governance are consistent with privacy law.

## 6.4 Contracted agencies

A responsible representative of every company contracted for any service which necessitates accessing personal health information should sign an undertaking to comply with the *HRIP Act* or equivalent law as part of the conditions of their contract. The agreement should clearly set out responsibility for data security in transit and requirements for secure storage. Consideration could also be given to the individual employed contractor workers signing such undertakings.

Examples of key privacy criteria appropriate for inclusion in any such contract are set out in Appendix 3.

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

## 6.5 Compliance tips

There are a number of ways health services can support their staff to meet the obligations under the *Act*. Some options include:

- Establish a Privacy Advisory/Working Group to oversee privacy management within the health service (to include Privacy Contact Officer, Privacy Project Officers, Privacy Training Coordinator, Health Information Manager, other interested staff).
- Encourage the revision of the pro forma 'Privacy leaflet for patients' for specific services, eg mental health, cancer care, palliative care, drug and alcohol, etc (see Appendix 5).
- Provide Information sheets/posters for staff providing contact details for privacy enquiries. Ensure that all staff know to liaise with their Privacy Contact Officer regarding requests for internal review.
- Include privacy training/education in staff orientation, and in staff handbook or 'Survival Manual' for new staff.
- Develop standard privacy undertakings for staff and student access to client/patient records (see Appendix 3).
- Reinforce importance of accurate documentation in health record and compliance with State Records legislation.

NSW Health Privacy Intranet site. The privacy intranet site contains resources to assist health services with interpreting and complying with privacy law. Key privacy resources available are:

- NSW Health Privacy Manual.
- Privacy Leaflet for Patients.
- Privacy Training Module.
- Privacy Newsletter.
- NSW Health Privacy Management Plan.
- Link to *Privacy and Personal Information Protection Act 1998.*
- Link to *Health Records and Information Privacy Act 2002*.
- Statutory Guidelines.

**The privacy intranet website is**
http://internal.health.nsw.gov.au/legal/Privacy.

# 7 Collecting personal health information

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 information.

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

While privacy laws impose some controls over when personal health information can be collected, these will not affect the core business of NSW Health.

The laws clearly allow health services and health service providers to collect personal health information for purposes relating to health care and treatment.

Health services are established under the *Health Services Act*. 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 client/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 training and education 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 can only be collected if the purpose of collecting is directly related to what the agency does and the collection is necessary for those purposes.

**Example**: Collecting details of a client's income is unlikely to be necessary for provision of public health services. Collection of information about pensioner or veteran status may however be necessary, if this information impacts on client/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 listening 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**
- 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. Particular care should be taken when it is clear the information may be personal, distressing or embarrassing to the client concerned.

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

**Example**: Doctors in a crowded emergency department request information from a client/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, regardless of the fact that 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 on the basis of 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.

Common examples of where it may be **unreasonable or impracticable** to collect personal health information directly from the client/patient include:

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

Where client/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 after a road 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 service provider as part of a referral.

## 7.4 Informing people 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, who by, 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 below.

#### 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, it can be given to an 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 the right to be told

If the client/patient expressly waives their right to be told, HPP 4 does not need to be complied with. HPP 4 requires this consent to be an "express consent", so any such waiver should be recorded to enable later verification.

#### 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, 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 client, yourself or another person at risk

**Example**: You do not need to inform a parent that a DOCs report has been made if there is an immediate risk that the parent may remove a child from a health service or that the child's safety may be at risk.

#### 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
- was collected in the process of recording a family, social or medical history, and this was necessary to provide health services to the client
- is collected from an authorised representative because the health service believes that the individual is incapable of understanding the nature of the information required
- 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 health service.

When information should be provided in these circumstances is governed by Statutory Guidelines issued by the NSW Privacy Commissioner.

### 🕮 Further guidance:

- Statutory Guidelines on notifying a person when you have collected health information about them from someone else at: www.lawlink.nsw.gov.au/privacynsw

### 7.4.2 What do they need to be told?

- identity of the health service collecting the information and how to contact them
- purposes for which the information is collected
- who the health service usually discloses information of that kind to
- laws that requires the particular information to be collected
- they are able to request access to the information
- main consequences, if any, for them if all or part of the information is not provided.

### 7.4.3 When should they be told?

The information should where practicable be given to clients 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 subsequently.

### 7.4.4 How should they be told?

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

- 'Privacy leaflet for patients' (see Section 7.4.5) to be made available to all patients
- verbal reinforcement or explanation of 'privacy leaflet for patients' where necessary
- privacy poster and counter notices displayed in public areas of hospitals and community health services
- information included on admission forms
- information provided on the health service's website.

**This information should be prominently displayed and readily and easily accessible to patients, both in admission areas, community health reception areas and within hospital wards.**

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 file to ensure a contemporaneous record is kept of the information provided.

### 7.4.5 Privacy leaflet for patients

A pro forma leaflet is provided in Appendix 5 setting out the information to be provided to patients, which must be presented in a format and in language that they can understand.

The 'Privacy leaflet for patients' is available in 29 community languages via the privacy intranet site, or via the Multicultural Health Communication Service website at: www.health.nsw.gov.au/health-public-affairs/mhcs/.

The pro forma leaflet is a general guide, and should be adapted by health services as appropriate 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 client/patient expectations to address. Examples of such services include, but are not limited to, cancer treatment, palliative care, mental health, drug and alcohol, sexual health, child protection and genetics services. 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). It should also be sufficiently clear to allow the client/patient to readily assess and understand the circumstances when client/patient information may be shared, for example whether it is shared with a wider treating team.

Circumstances for sharing client/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 brochure health services should contact the NSW Department of Health to ensure the adaptations remain within these parameters. Consideration also needs to be given to ensure appropriate translations are available.

### 🕮 Further guidance:

- Section 7.4.2: What do they need to be told?
- Section 11: Use and disclosure of personal health information
- Appendix 5: Pro forma privacy leaflet for patients

# 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 an organisation.

Patients may seek to obtain services anonymously in cases where sensitive issues arise, such as counselling and drug use issues, or attending sexual health clinics. Health services may provide specific clinics to deal with these issues.

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

## 8.1 When may providing a service anonymously be impracticable?

There may also be a range of circumstances where providing services anonymously may be impracticable. For example:

- a service may require follow-up. If the person does not provide details to allow this, the ongoing care may be compromised
- the care to be provided involves a multi-disciplinary team, making it difficult to provide ongoing care without a clear identification of the client/patient
- anonymity would deny a clinician information critical to providing safe and appropriate care, a client/patient's medical status may be compromised
- concerns may also arise that providing services anonymously may, in some situations, lead to an increase in the health service's liability.

## 8.2 When may providing a service anonymously 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 (eg accessing free care in an emergency/outpatients setting)
- Department of Veterans' Affairs entitlements require the provision of actual name
- 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 medical practitioner is required to record certain details, including identity, to allow the matter to be reported to the NSW Department of Health.

# Retention, security and protection (HPP 5)

# 9

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 should be retained.

Health services should therefore refer to the General Disposal Authority (GDA 17) Public health services: Patient/Client Records, issued by State Records NSW in determining how long to retain clinical and client/patient records.

### 🕮 Further guidance:

- General Disposal Authority No.17: Public health services: Patient/client records (available from state records NSW at www.records.nsw.gov.au.
- PD2005_127: Principles for creation, management, storage and disposal of health care records.

## 9.2 Security of personal health information

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

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

### 🕮 Further guidance:

- PD2005_314: Electronic information security policy
- NSW Premiers circular No. 2001-46.

### 9.2.1 Paper records

*Storage*: All paper records containing personal health information should be kept in lockable storage or secure access areas when not in use. Basic precautions such as not storing records containing personal health information in a public area should not be overlooked. Care should be taken not to leave documents containing personal health information on work benches or anywhere they may be visible to unauthorised people.

*Disposal*: Paper records containing personal health information should be disposed of by shredding, pulping or burning. Where large volumes of paper are involved, specialised services for the safe disposal of confidential material should be employed.

### 9.2.2 Computer systems and applications

As at June 2005, the NSW Department of Health was developing more detailed policies to set security rules for computer systems and applications, including the eMR (electronic medical record) and the eHR (statewide electronic health record, or Health eLink).

The material provided below offers some options which health service providers may consider to maximize security of these systems, and should be read subject to the specific NSW Health policies on security of information stored in an electronic environment.

*Storage*: A secure physical and electronic environment should be maintained for all data held on computer systems in accordance with NSW Health and NSW Government policies listed at 9.2. Consideration could be given to providing different staff with different levels of access (ie, full partial or no access).

*Disposal*: Disposal of data records should be done in such as way as to render them unreadable and leave them in a form from which they cannot be reconstructed in whole or in part.

### 🕮 Further guidance:

- http://internal.health.nsw.gov.au/im/.
- http://internal.health.nsw.gov.au/im/ibs/ehr.
- http://internal.health.nsw.gov.au:2001/emr.

### ☎ Contact:

The Strategic Information Management Branch (SIM)
NSW Department of Health
Tel. (02) 9391 9000

## 9.2.3 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 minimal standards should be applied when providing the information.

Requirements necessary to maintain secure delivery will vary depending on the medium of transmission of the information.

#### 9.2.3.1 Telephone

No personal health information, including admission and discharge dates, should be given over the telephone unless it has been established that the caller has legitimate grounds to access the information and can give proof of identity.

- Only those authorised by the health service should give client/patient information by phone; it is a matter for local determination which health workers should be so authorised.
- No personal health information should be left on voice mail. The caller's or the clinician's name and contact number may be provided where the client/patient is likely to recognise the name. Otherwise, the name of the health service may be provided, or where sensitivities arise, the name of the Area health service, or equivalent, should be used.

#### 9.2.3.2 Facsimile

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 persons granted access can access documents
- fax cover sheets should carry an appropriately worded privacy notice. See Appendix 4 for sample wording
- 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
- call the recipient to advise them that you are about to send a fax and that they should call you back if they do not received the fax.

#### 9.2.3.3 Mail

- Packaging of mail and courier items should be secure and care should be taken that addresses are complete and correct.
- Mail should be marked 'Confidential: Attention ...'
- It is the responsibility of the staff member who receives mail and courier items to ensure that these are kept in a secure location to prevent loss and unauthorised access until they have been delivered to the addressee.

#### 9.2.3.4 Electronic discharge referrals/summaries

NSW Health has a number of systems which automatically generate electronic discharge referrals/ summaries (eDRS) to external health service providers (such as general practitioners, specialists and allied health service 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 service providers should:

- have processes in place to ensure 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 for client/patient admissions

- 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 admission personnel 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.

#### 9.2.3.5 Other electronic transmission, including email

Health services must take steps to safeguard their electronic information and to prevent inappropriate access. Outside the transmission of electronic discharge referrals/summaries (as set out in 9.2.3.4), transmission of personal health information via email within health services should be restricted to wherever it is essential for immediate ongoing care. In addition, the following precautions should be taken:

- only include client/patient information which you know to be required for the purpose
- ensure you have the correct email address. Wherever practicable, request that the recipient provides you with their email address by emailing you first
- take particular care not to inadvertently copy unintended recipients on the email.

The NSW Healthnet (NSW Department of Health and area health service intranets) are generally secure for the transmission of information. As at June 2005 the NSW Department of Health was in the process of developing guidelines for the use of internet/email outside this system, or via non-encrypted means.

### 🕮 Further guidance:

- Section 16: Electronic health records.
- PD2005_314: Electronic information security policy.
- NSW Premiers circular No. 2001–46.
- NSW Premiers circular No. 2004–06.

### 9.2.4 Printing and copying

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

Where practicable, identifiable information should be blocked out on the copied record.

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.

### 9.2.5 Training and demonstrations

The anonymity of clients/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 client/patient has been obtained.

Identifiable and potentially identifiable information can be used for some training purposes, including those involving clinical placements.

### 🕮 Further guidance:

- NSW Privacy Commissioner's Statutory Guidelines on training: www.lawlink.nsw.gov.au/privacynsw.

### 9.2.6 Conversations

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

### 9.2.7 Visibility of screens

Computer screens which display personal health information in public areas should, where possible, be so placed that they cannot be seen other than by the staff member entering the information.

If left unattended, no personal health information should be left on the screen. Screen savers and passwords should be used where possible to reduce the chance of casual observation.

# 10 Accuracy (HPP 9)

HPP 9 deals with accuracy of 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 records is a critical aspect of health service provision. The health record is a critical part of treatment planning and decision making. It is critical 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 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 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
- 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
- patients should be notified of amendments to their record where appropriate
- the treating health care provider should periodically review the record for correctness
- there should be an audit trail for electronic records.

### 🕮 Further guidance:

- PD2005_127: Principles for creation, management, storage and disposal of health care records.
- Australian Standard for electronic systems AS7799.

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

11

In general terms, a '**use**' of personal health information refers to the communication or handling of information within a health service.

A '**disclosure**' refers to the communication or transfer of information outside a health service. A disclosure can occur through:

- giving a copy of the information to another organisation or individual
- allowing another organisation or individual to have access to the information
- giving out summaries, or communicating the information 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 client/patient.

Use and disclosure are treated together as privacy law generally imposes the same conditions on both activities. The one exception is that the disclosure provisions also allow disclosure on compassionate grounds (see 11.2.9), this 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
- where information is used or disclosed for another "secondary purpose", and one of the criteria listed in the HPPs applies
- where the use or disclosure of the information is lawfully authorised.

Activities which fall outside of these three categories, are not permitted without client/patient consent unless a special exemption pursuant to Section 62 of the *HRIP Act* is obtained. Section 15 provides guidance on how to address some of these issues, including requests for media access (see 15.7) and fund raising (see 15.8).

## 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 collecting purpose will be to provide care, or an episode of care.

**Example**: 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, eg health service providers including nursing staff, anaesthetists and pathologists.

**Example**: 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 fund raising was not the "primary purpose" for which this information was collected, this use could only proceed if it were an authorised secondary purpose under the privacy laws.

## 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 to 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 11.2.1)
- use or disclosure to which the individual has consented (see 11.2.2)
- use or disclosure to prevent a serious threat to health or welfare (see 11.2.3)

- use or disclosure for management, training or research purposes (see 11.2.4)
- use or disclosure to assist in finding a missing person (see 11.2.5)
- use or disclosure as part of investigating and reporting wrong conduct (see 11.2.6)
- use or disclosure to or by a law enforcement agency or investigative agency (see 11.2.7 and 11.2.8)
- disclosure made on compassionate grounds (see 11.2.9).

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

## 11.2.1 Directly related purpose

**HPP 10 &11(1)(b)**

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

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

Directly related purpose often arises in the health system, in particular in relation to sharing information with other health service providers (See 15.1 – Third party health service providers).

### 11.2.1.1 "Directly related purpose"

This recognises there are activities necessary, such as provision of ongoing care, billing and following up test results which may not fall within the primary purpose for which the information was collected.

What will be 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
- disclosing information to another person or organisation involved in the ongoing care of the client/patient
- sending reminders to a client/patient where the person receives a service on a regular basis or requires a follow-up service
- maintaining lists of client/patient names for client/patient care and safety purposes. Examples include community health client/patient lists, client/patient lists for fire evacuation (for use by the fire brigade in event of an emergency), etc.
- using information for quality assurance or clinical audit activities carried out by the health service such as monitoring, evaluating, auditing the provision of the particular product or service the health service has or is providing the person (including compliance with the NSW patient safety and clinical quality program)
- disclosing information to an auditor or quality assessor for the purposes of monitoring, evaluating, 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 records is bound by privacy legislation or a professional code of ethics)
- using the information to investigate complaints about care provided by the health service or client/patient safety
- using the information to manage the provision of the service or product
- disclosing information to enable follow-up of complaints about the service or a product, or recalls of a product
- administrative activities associated with providing, following up on or receiving payment for the service or product and follow-up on an overdue payment (this would allow disclosures to a debt collector)
- using or disclosing information in the course of managing a legal action or claim brought by the client/patient against the health service.

This can also include other functions of the health service, such as management or research (see 11.2.4).

**Example**: An antenatal unit from another hospital is requesting a copy of the notes relating to the client/patient's 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 been discussed this issue with the patient or her authorised representative prior to making the request.

#### 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 client/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 client/patient or client at the time of collection thus becomes important.

If you make it clear to the person as part of the collection process that their information may be used or disclosed for these purposes, then there is a more persuasive argument that the person would 'reasonably expect' you to use or disclose their information in these ways.

Section 7 of the manual sets out the types of information that needs to be provided and the ways it may be given. Appendix 5 provides a pro forma privacy leaflet for patients.

#### 11.2.1.3 Outside client/patient's "reasonable expectation"

In rare circumstances, a client/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 client/patient's health care (see 11.2.1.1).

When health service staff receive such a request, it will be situation specific and the professional judgement of local health service staff will be required to resolve such requests. To assist staff in reaching a judgement, the following guidance is provided.

1. A senior clinician should consider whether it is reasonable and practicable to meet the client/ patient's request without putting the client/patient, staff member or any other person at risk of harm. Wherever it is possible to meet the client/patient's request, reasonable steps should be taken to comply with the request, and this should be documented in the client/patient's health record.
2. Where it is not possible to comply with a client/ patient's special request, a senior clinician (and other health service staff as necessary) should discuss with the client/patient:
   a. reasons for the client/patient's concerns about sharing the information
   b. reasons why there is a need to share information with all health service staff involved in their care
   c. obligations all staff have under privacy law to ensure all personal health information is kept confidential
   d. consequences on the client/patient's health care if personal health information is not shared.
3. If the client/patient's remains of the view that they wish information to be withheld and it is the opinion of the treating 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 client/patient is prepared to consent to the treatment itself. The service provider should explain this to the client/ patient and that the facility is unable to provide health services to the client/patient given this effective refusal. Where appropriate, the facility may wish to offer to refer the client/patient to another facility, or suggest that the client/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 client/patient to resolve the issues and should also contact the privacy contact officer for their health service to liaise with the client/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 Key Concepts, Section 5.4. Consent.

#### 11.2.2.1 Where a third party seeks access

The need for a consent may arise because a third party has sought access to the client/patient's records. A client/patient can consent to, or authorize any third party, such as a relative, interpreter, medical practitioner (not involved in their ongoing care), legal representative, employer, insurer or officer, to have access to his or her health record. Members of parliament making representations on behalf of a constituent are also required to have authorisation.

The procedures which should be followed in such cases are set out below.

**Form and content of consent**

The client/patient's consent should be in writing (not a photocopy, except as outlined below). It should be signed by the client/patient or their parent or legal guardian and should contain:

- full name of client/patient
- date of birth
- present address and, if different, address at the time of the health treatment in question
- date of written consent (see Section 5.4.1, Elements of Consent)
- details of the records/information in question
- range of dates for health treatment in question
- name of person being authorised and their relationship to the client/patient
- the purpose for which the information is requested (where relevant).

Photocopies of consent authorities are not sufficient unless they are from a client/patient's insurer (see below).

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.

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 by the client/patient, containing the client/patient's consent to disclosure, is sufficient authority for the release of a medical report or summary of injuries. Other information should not be provided without the clearly documented written consent of the client/patient.

**Proof of identity**

Two forms of identity should be sighted, such as driver's licence, health benefits card, etc, preferably with a photograph. If the person does not seek access in person, they should be required to provide specific information to confirm their identity.

**Conditions of access**

Access should generally be provided by direct access, or viewing of the record on the health service's premises. A health care provider or health information manager should always supervise access.

When copying records for legal purposes, employees should be aware of the requirements of the *Evidence Act 1995*.

**Fees and charges**

Where the person requests to have copies of the health record made, the fees and charges set out in PD2005_235: Charges for health records and medical reports.

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

#### 11.2.2.2 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 client/patient has adequate capacity to give consent (see 5.4)
- address the elements of consent outlined in 5.4
- make a written record of the consent, either through a written consent form signed by the client/patient, or by a contemporaneous note of a verbal consent recorded in the file.

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

- A written consent is the strongest evidence that the client/patient has given their consent, and so would normally be obtained at admission, on commencement of the therapeutic relationship, or where there are many or complex issues the client/patient needs to consider before consenting.

- 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 (such as, eg fundraising, see 15.8).
- Written consent is not required for day-to-day disclosures relating to ongoing care and treatment, or actions covered by an existing written consent.

### 11.2.3 To prevent a serious and imminent threat to health or welfare

**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
- serious threat to **public health or public safety**.

#### 11.2.3.1 General guidelines

Health workers 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 care provider considers that a client/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 colleagues or a senior health care provider before acting.

**Example**: a client of a community health service arrives in an agitated state, making threats against a close family member over a custody dispute, and leaves. The client 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 and imminent risk, and so could disclose the information in order to address this risk.

**Example**: a patient is critically ill, requiring urgent surgery and the clinicians need details of past anaesthetics to enable them to proceed with the surgery.

**Example**: a Public Health Unit conducting an investigation 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.

#### 11.2.3.2 Where staff may be at risk

Sharing of information about a client/patient's violent behaviour is permitted when the client/patient is referred or transferred within or between facilities, and when the client/patient poses a threat to themselves or any individual including staff, or to public health or public safety. Key principles to managing violent behaviour are:

1. Privacy obligations must be balanced with health service's obligations to ensure a safe workplace under the *Occupational Health and Safety Act*.
2. Relevant client/patient information should be made available when referring or transferring a client/patient to ensure client/patient and staff safety during transfer and to prevent adverse incidents.
3. When sharing information about a client/patient, focus on client/patient behaviours that may pose a threat or risk, and appropriate client/patient management strategies.
4. A health service must take reasonable steps to ensure the information they share is relevant, accurate, up-to-date, complete and not misleading.
5. Use client/patient alerts or client/patient flagging in accordance with Section 7.3 of the 'Zero tolerance: response to violence in NSW Health workplace'.

### 🕮 Further guidance:

- PD2005_315: Zero tolerance – response to violence in NSW Health workplace.
- PD2005_409: NSW Health workplace health and safety – policy and better practice guide.
- PD2005_339: Protecting people and property – NSW Health policy and guidelines for security risk management in health facilities.

### ☎ Contact:

Employee Relations Unit
NSW Department of Health
Tel. (02) 9391 9305

#### 11.2.3.3 *Public Health Act* – Notification of public health risk for HIV

Under the *Public Health Act* strict limitations are imposed on the disclosure of information indicating a person's HIV status, and information that a person has undergone a HIV test (see 4.1.3). The authorised disclosures under this *Act* generally relate to treatment or other required disclosures.

The *Public Health Act* however also allows for the disclosure of information relating to a person's HIV status where the failure to provide the information could place the health of the public at risk. The disclosure provision is limited and only allows notification of the Director-General of the NSW Department of Health. It does not authorise disclosure to any other person.

Section 17 places strict limitations on the release of this information, which can only be disclosed:

- to a person involved in the care or treatment or counselling of the person to whom the information relates, if the information is required in connection with that care
- with the consent of the person to whom the information relates
- in connection with the administration of an *Act*
- under an order of a Court or a person authorised to examine witnesses.

If staff are concerned about a possible health risk relating to HIV or the behaviour of a HIV positive person, they should contact their local HIV coordinator or the AIDS and Infectious Diseases Branch of the NSW Department of Health.

### 🕮 Further guidance:

- Section 15.9.5: Managing public health risks.
- PD2005_184: Contact tracing guidelines for sexually transmissible diseases and blood borne viruses.

### 11.2.4 Management, training or research

**HPPs 10 & 11 (1)(d), (e) &(f)**

A health service may use or disclose personal health information if this is reasonably necessary for:

- **funding, management, planning** or evaluation of health services
- **training** the health service's employees or people who work with the health service
- research or the compilation or analysis of statistics in the public interest
- the use or disclosure is in accordance with **Statutory Guidelines** issued by the NSW Privacy Commissioner.

#### 11.2.4.1 When to use this exemption

Many funding, management, and planning purposes will be a "directly related purpose" (see Section 11.2.1), so you should first check if that exemption applies before considering these exemptions. Each of the exceptions 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. De-identified information cannot be re-identified.

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 you need identified information 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 '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 re-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.

**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.

### 11.2.4.2 Statutory Guidelines

The Privacy Commissioner has issued Statutory Guidelines that set out conditions imposed on use and disclosure of personal health information for management, research and training.

**Management Guidelines**

The Management Guidelines discuss each of the preconditions in detail, and draws attention to the relevant "directly related purpose" which may otherwise apply. The Guidelines then provide for a Health Research Ethics Committee to consider the proposed use or disclosure and assess whether, on balance it is in the public interest.

To view Guidelines go to:
www.lawlink.nsw.gov.au/privacynsw

**Research Guidelines**

The Research Guidelines are consistent with and mirror the Guidelines developed by the NH&MRC under sections 95 and 95A of the *Commonwealth Privacy Act*. Research requiring use or disclosure of personal health information will need to be considered by a Health 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 where de-identification would defeat the purpose of the training. The Guidelines then set requirements for managing such training.

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

**Training and demonstrations**

The anonymity of clients/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 client/patient has been obtained.

**Clinical placements and students:**

Student health professionals must sign a Privacy Undertaking (see Appendix 3), and must comply with privacy law and all NSW Health policies.

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 records off-site. Clients/patients may refuse to have a student participate in their treatment.

### 11.2.5 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 entitled to provide this information under this provision.

### 11.2.6 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 a health registration *Act*, or conduct by an employee 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 activities.

The exemption allows use or disclosure of the information necessary for the health service to investigate or report the conduct in question. It covers information to be:

- provided to the Health Care Complaints Commission or a Health Professional Registration Board
- provided to Units of the NSW Department of Health which may conduct investigations into breaches of legislation, including the Pharmaceutical Services Branch, Employee Screening and Review Branch
- shared between these investigative units within NSW Health.

### 11.2.7 Law enforcement agencies, including police

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

HPP's 10 and 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 are reasonable grounds to believe that an **offence may have been or may be committed**.

#### 11.2.7.1 What is a "law enforcement agency?"

The *HRIP Act* 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.
- NSW Department of Corrective Services.
- Department of Juvenile Justice.

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

The law enforcement exemption under HPP's 10 and 11 is very broad. It covers any information relating to an offence which has or may be committed, provided that 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, having regard to:

- the seriousness of the offence involved. For example, does it involve an offence involving serious physical harm such as attempted murder, assault (including gunshot wound) or domestic violence?
- 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 11.2.3).
- the impact of the disclosure on client/patient care and the therapeutic relationship. The nature of the service being provided and the potential that the client/patient may discontinue obtaining care and treatment, should be considered, as well as the possible impact on the client/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. For example NSW Health Domestic Violence policies require the reporting of suspected domestic violence to the police.

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

**Any other information may only be provided with client/patient consent or in response to a search warrant.**

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

Requests should be in writing, identify the requesting officer (eg, in the case of police, including badge number) and confirm 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 over the phone unless in response to a previous written request or where the requesting officer's identity can be verified.

Requests should be dealt with by the treating health service 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 record
- where clinical information is necessary, this should be limited to a general outline of the client/patient's condition and/or injuries.

**Example**: An ambulance officer attends a male 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 ambulance officer's opinion the patient is medically competent to be interviewed. The ambulance officer 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. Ambulance officers are not required to discuss other matters relating to the patient, such as whether they are competent to be interviewed.

### Further guidance:

- 11.2.3: To prevent a serious and imminent threat to health or welfare.
- 11.3.4: Reporting serious criminal offences.
- 15.2: Requests from State and Federal Police.

### 11.2.8 Investigative agencies

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

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
- Independent Commission Against Corruption
- Police Integrity Commission, the Inspector of the Police Integrity Commission and any staff of the Inspector
- Health Care Complaints Commission
- Office of Legal Services Commissioner.

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

- 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
- provide access only to information that is relevant and necessary for the purpose
- document all instances of access in the record
- where appropriate and practicable, inform the individual to whom the information relates of the access.

### 11.2.9 Disclosure on compassionate grounds

**HPP 11(1)(g)**

A health service may disclose 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.

An immediate family member includes an individual person who is a:

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

This exemption is most likely to arise in emergency situations, or in cases where a person has died. Personal health information remains covered by privacy principles until 30-years after a person has died.

The exemption is restricted as follows the :

- disclosure must be limited to "what is **reasonably necessary**" for those reasons
- individual must be **incapable of giving consent**
- 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.

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

**Example**: a young person is admitted to hospital unconscious and seriously ill, they have no identification but their mobile phone 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.

**Example**: a person has died suddenly at hospital without indicating his views 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.

**Example**: 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.

## 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 that is required by the authority, no more and no less
- check if PD2005_235: Charges for health records and medical reports 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 the statutory power

There are many such statutes, but some examples of those which commonly apply to a health service are set out in 11.3.1 to 11.3.12 below.

### 11.3.1 NSW Department of Health Officers and Environmental Health Officers

NSW Department of Health officers have powers under the *Health Services Act*, *Private Hospitals and Day Procedure Centres Act* and *Nursing Homes Act* to obtain information. Inspectors carry authorisations that indicate the nature of their powers and confirm their authority.

Environmental health officers from public health units have powers under the *Public Health Act* to obtain information. Inspectors carry authorisations that indicate the nature of their powers and confirm their authority.

### 11.3.2 Department of Community Services (DoCS)

The *Children and Young Persons (Care and Protection) Act 1998* contains a range of information sharing and disclosure provisions designed to assist the Department of Community Services exercise its statutory child protection functions. The key provisions are listed below.

**Section 27: Reporting children at risk.** Health workers are required to report to the Department of Community Services cases where they have "reasonable grounds to suspect that a child is at risk of harm".

**Section 248: Information sharing with DoCS**. Allows DoCS to request a health service provide information "relating to the safety, welfare and well-being of a particular child or young person or class of children or young persons".

**Section 173: Medical examinations**. Where a medical examination has been conducted in accordance with Section 173, the information obtained may be disclosed to the Director-General of DoCS or a delegated officer.

**Further guidance** on Child Protection:

- PD2005_299: Protecting children and young people.
- Frontline Procedures for the protection of children and young people (2000).
- NSW Interagency guidelines for child protection intervention.

All documents available at:
http://internal.health.nsw.gov.au/policy/hsp/child-protection.html.

**Contact:**

Child Protection & Violence Prevention Unit
NSW Department of Health
Tel. (02) 9424 5825

### 11.3.3 Prison officers (access to health records of prisoners)

The staff of Justice Health may disclose information relating to the medical history of a prisoner to a prison officer duly authorised by the gaol superintendent to investigate an incident or assault involving that prisoner. justice health staff must, in these circumstances, complete the document entitled Justice health service Incident/Assault form.

Sharing of Information between Justice Health and the Department of Corrective Services is dealt with by a memorandum of understanding. Requests from other correctional facilities for health information should be in writing indicating the basis of the authority for disclosure (such as directly related purpose, consent etc – for detail, see Section 11.2.1).

### 11.3.4 Reporting "serious criminal 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 an offender. 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 two-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 workers should be aware that this covers offences such as drug trafficking, serious assaults, sexual assaults, murder and manslaughter. It does not cover minor possession offences or any offences under public health legislation.

The Regulations under the *Crimes Act* also provide that a prosecution for an offence under this law will not to be commenced against a person without the approval of the Attorney General if the information was obtained in the course of practising as a:

- medical practitioner
- psychologist
- nurse
- social worker, including, a support worker for victims of crime, and a counsellor who treats persons for emotional or psychological conditions suffered by them
- researcher for professional or academic purposes.

The aim of the provision is to protect health service providers who, in good faith and on reasonable grounds, do not disclose this information to police.

NSW Health has issued a range of policies which provide guidance on the obligations established by Section 316. Interagency guidelines for responding to adult victims of sexual assault, jointly issued by the NSW Department of Health, the police and the Director of Public Prosecutions, establish protocols and procedures for all issues dealing with sexual assault, including reporting. Health workers are referred to that policy for guidance on appropriate action.

### 📖 Further guidance:

- Section 11.2.7: Disclosure of information to law enforcement agencies.
- PD2005_413: Identifying and responding to domestic violence.
- Sexual Assault Services Policy and Procedure Manual.

### ☎ Contact:

Child Protection & Violence Prevention Unit
NSW Department of Health
Tel. (02) 9424 5825

## 11.3.5 Coroner

The *Coroner's Act 1980* requires notification to the Coroner of deaths occurring under certain conditions.

Health records required for post-mortem examinations must also be provided to the Coroner.

Where a post mortem is to be conducted the pathologist or medical officer conducting the post mortem should also have access to the health record.

When health records are tendered to the Coroner, the treating health care provider should be notified.

### 📖 Further guidance:

- PD2005_352: Coroners' cases and amendments to *Coroners Act 1980.*

## 11.3.6 Search warrants and subpoenas

**Search warrants**

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.

**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 coordinate responses to subpoenas.

Where a client/patient whose health record has been subpoenaed is not named as a party to the proceedings, he or she 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
- oppression (where the terms of a subpoena are excessively wide and imprecise)
- public interest immunity
- legal professional privilege
- sexual assault communications privilege.

If a health worker 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.

If acceptable, copies should be provided and the original record retained by the health service. Where originals are required, the 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. A receipt signed by the official receiving the record should be obtained which specifies the record number, date received and name of the Court.

### 📖 Further guidance:

- PD2005_405: Subpoenas.

### 11.3.7 Health Care Complaints Commission

#### 11.3.7.1 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 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.

#### 11.3.7.2 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.

### 11.3.8 The Ombudsman

The Ombudsman is empowered to require health authorities to supply information where a formal investigation is being conducted under the *Ombudsman's Act 1974*, and investigates reviewable child deaths.

No information should be provided without prior reference to the Department's Complaints Manager in the Executive Support Unit.

### 11.3.9 Official visitors

Official visitors are appointed under the *NSW Mental Health Act* to inspect psychiatric hospitals.

Under Section 231(1)(d) of the *Act* official visitors must be provided with access to records relevant to the care of patients.

### 11.3.10 Child Death Review Team

The NSW Child Death Review Team and the Ombudsman review child deaths that occur in suspicious circumstances or are associated with suspected abuse or neglect.

Under Section 45T of the *Commission for Children and Young People Act 1998* the Team has powers to obtain unrestricted access to relevant health records and to obtain copies on request.

### 11.3.11 Workcover

Section 62 of the *Occupational Health and Safety Act 2000*, allows Workcover to require production of material relevant to the investigation of an alleged breach of the *Act*. Such a request must be made either in writing stating the reasons why access is being sought, or a formal Section 62 notice should be issued.

### 11.3.12 Commonwealth Agencies

#### 11.3.12.1 Family and Community Services

The Commonwealth Department of Family and Community 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*.

#### 11.3.12.2 Veterans' Affairs

Under Section 128 of the *Veterans' Entitlement Act* the Department 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.

Disclosure of client/patient information for purposes other than funding are subject to the exemptions listed in 11.2. Disclosure of the names of DVA patients for the purpose of visits by voluntary groups is only permitted with client/patient consent.

Deaths of repatriation clients must also be reported to the Department of Veterans' Affairs.

#### 11.3.12.3 Immigration and Multicultural and Indigenous Affairs (DIMIA)

The Department has powers under Section 18 of the *Migration Act 1958* (Cth) to obtain information about illegal non-citizens.

The power allows the Department of Immigration and Multicultural and Indigenous Affairs (DIMIA) 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 unlawful non-citizen. The power must be exercised by service of a notice in writing.

### 11.3.13 Statutory reporting requirements

The public health system is required by legislation to notify authorised agencies of certain types of personal health information.

***Public Health Act***

- Scheduled Medical Conditions.
- Inpatient statistics.
- Maternal and perinatal data for Midwives Data Collection.
- Cancer cases (through the NSW Cancer Registry).
- Data for Birth Defects Register.

must be reported to the Department of Health

### Further guidance:

- 15.9.5 *Public Health Act*

***Health Services Act***

- Chief Executives of health services have an obligation to report suspected unsatisfactory conduct or suspected professional misconduct of employees or contracted service providers (VMO's) to the relevant health professional registration board.

***Registration of Births, Deaths and Marriages (Amendment) Act***

- Perinatal deaths must be reported to Principal Registrar.

***Health Services Act, Private Hospitals and Day Procedure Centres Act***

- Adverse drug reactions must be reported to the Australian Drug Evaluation Committee Department of Health.

## 11.3.14 Information required by the Minister or Premier

NSW privacy laws also recognise that from time to time the executive arm of government (ie 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 or restricts 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
- 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.

# Patient access and amendment (HPPs 6,7 & 8) 12

## 12.1 Access to personal health information (HPPs 6 & 7)

The *HRIP Act* also allows a person to obtain 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 seek access to that information.

Health services are required to inform clients of these options at the time information is collected (See Section 7).

## 12.2 Interaction of *HRIP Act* and *FOI Act*

The general principle under both privacy and FOI laws is that **a person will be presumed to have a right to access their own files**. This also reflects NSW Health policy since at least 1989.

The *HRIP Act* recognises however that sometimes circumstances will arise where granting 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 was designed to recognise circumstances where access could be refused under the *Freedom of Information Act.*

Section 31 of the *FOI Act* allows access to be refused to documents if their release would affect the **personal affairs of any person**. The Section specifically includes medical or psychiatric information concerning the applicant where the release may have an adverse impact on their physical or mental health. This would also cover a request by parent or guardian where there are reasonable grounds for believing that access may lead to child abuse or be prejudicial to the child's physical or mental health. When access is sought, staff should carefully review the fine to ascertain if these issues arise.

If access can be refused on this basis under the *FOI Act*, the health service will be "lawfully authorised" to refuse access under the *HRIP Act*.

There may also be other grounds for refusal in the *FOI Act*. Staff should check with their local FOI coordinator.

**Example**: A father has applied for access to personal health information relating to his 6-month old child, however, there is an AVO against the father not to go near the child. Privacy law and the *Freedom of Information Act* allow for access to be refused where this may put a person at risk of harm, or where access may be prejudicial to the child's physical or mental health.

## 12.3 Process for determining access

In circumstances where the treating health care provider considers access could be prejudicial to the physical or mental health of the client/patient (and this would be a rare occurrence), the health record should be referred to a third party such as an independent medical practitioner.

The health record plus the assessment should then be referred to the senior health care provider for review and a decision on whether the client/patient should be granted access to all or part of his/her record.

Where access is granted but there remains a concern as to the impact the information may have on the client/patient, a written warning to this effect should be given to the client/patient, and a copy included on the record.

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 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, and therefore access to the record.

Where access is being requested to reports made to DoCS, the identity of the staff member who made the report is privileged and must not be released.

## 12.4 Obtain proof of identity

If applying in person, two forms of identity should be sighted, such as driver's licence, health benefits card etc, preferably with a photograph. If applying by mail, photocopies can be accepted with written confirmation from the applicant that the copies are bona fide. Alternatively, the person should be required to provide specific information to confirm their identity.

## 12.5 Conditions of access

Access should generally be provided by direct access, or viewing of the record on the health service's premises. Clients may request the assistance of a health care provider in interpreting the record.

A health care provider or health information manager should always supervise access by a client/patient to his or her health records.

When copying records for legal purposes, employees should be aware of the requirements of the *Evidence Act 1995.*

Ideally, records should be reviewed prior to providing access to ensure no unauthorised material is provided, for example, information identifying a person who has made a child protection notification to DoCS.

## 12.6 Fees and charges

Where the person requests to have copies of the health record made, refer to PD2005_235: Charges for Health Records and Medical Reports.

The requirements and conditions imposed on client/ patient access mirror the requirements imposed on other third party access approved by the client/patient (See 11.2.2.1).

## 12.7 Additions and corrections

HPP 8 allows individuals to request a health services to make changes to their personal health information. HPP 8 provides that a change 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 record unless of the view it is necessary to do so in line with the above criteria.

Patients should be notified of the outcome of their request for amendment, and if amendment is refused, the reason for the refusal.

### 12.7.1 Where an alteration is included

Untraceable alterations or deletions should not be made. Original incorrect entries should not be erased but lined through so the original entry remains readable.

The reason for the amendment should be noted in the file and signed.

Nothing in these provisions should be taken to prevent the routine updating of demographic information such as address, contact details and patients general practitioner.

### 12.7.2 Where an alteration is refused

If the health service is not willing to make the requested changes HPP 8(2) requires it to **take such steps as are reasonable** to attach additional information to the record.

The client/patient's own comments should be attached as an addendum to the record on request, along with an explanation of the circumstances.

# Miscellaneous HPPs 13

## 13.1 Identifiers (HPP 12)

Identifiers are used by health services to uniquely identify an individual and their health records. While identifiers such as an MRN or UPI may not use a person's name and address, they are designed to be unique to a specific individual and hence will be "personal health information", and subject to the privacy laws.

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.

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
- 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.

## 13.2 Transferring personal health information out of NSW (HPP 14)

Health services frequently need to transfer personal health information to agencies and health services in other states, 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 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.

### 13.2.1 Within Australia

The current status of privacy policy or law means that sharing of information with health services in Australia can occur without consideration of the exceptions listed for HPP 14.

- 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.

### 13.2.2 Outside Australia

Countries in the EU are bound by the EU Directive on Information Privacy. As such, disclosure to these countries would comply with HPP 14.

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(2) 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 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 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 11.3).

## 13.3 EHR Linkage at state or national level (HPP 15)

HPP 15 does not affect the ability of health services to store or link personal health information electronically. Such storage and linkage should occur in line with the general terms of this manual and relevant NSW Health policies. HPP 15 is directed at EHR systems that link health records at a state or national level. It requires that such a system must be "opt-in", in that a client/patient must give "express consent" to participate in such a system. Any such consent must comply with the requirements outlined in 5.3 and must be in writing.

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
- where the linkage is for research purposes and has been approved in accordance with the Statutory Guidelines on Research.

Special exemptions may be sought from the Privacy Commissioner if there is adequate public interest argument for the development of an electronic health record that allows individuals to opt out rather than opt in to the system.

# Complaints handling 14

Health service should always try to resolve complaints quickly and informally, using formal processes as a last resort. However privacy law provides clients with a right to make a formal complaint.

The *Health Records and Information Privacy Act* requires health services to use the complaints process set out in Part 5 of the *Privacy and Personal Information Protection Act.*

Guidelines for management of complaints using these processes are set out in NSW Health Privacy Management Plan, Part 2 Internal Review Guidelines. If you receive a complaint under privacy legislation, you should refer to this document.

### 🕮 Further guidance:

- PD2005_554: NSW Health Privacy Management Plan, Part 2 Internal Review Guidelines.

## 14.1 General principles

Individuals can make a complaint about a health service's handling of personal health information privacy on the grounds that the health service has contravened a Health Privacy Principle or a Health Privacy Code of Practice.

A 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).

A person is not required to identify the particular HPP that he or she considers has been breached. Health services are under an obligation to review any such complaint received and to identify the specific HPPs which arise.

The privacy law provides first for a health service to conduct an internal review of a complaint.

If the complainant is not satisfied with this outcome, he or she may then appeal the issue to the Administrative Decisions Tribunal (ADT).

Where a person lodges an action before the ADT, the health service should notify the NSW Department of Health Legal and Legislative Services Branch of the application.

## 4.2 Sanctions

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
- refrain from any conduct or action in contravention of a HPP
- comply with a HPP
- correct information which has been disclosed
- take specified steps to remedy any loss or damage suffered by the applicant.

If the Tribunal finds a **public sector official** guilty of intentionally disclosing or using personal health information, it may order:

- the individual to pay a fine of up to $11,000 or to be imprisoned for up to 2 years, or both
- to confiscate any money or other benefit alleged to have been obtained by the individual in connection with the offence.

# 15 Common privacy issues

Sometimes health workers may have a short question about broader interaction with other government agencies, specific projects or matters that cut across the HPPs outlined in Parts 7–13. In recognition of this, Section 15 of the manual is designed to provide a Quick Reference Guide on common privacy issues in NSW Health.

## 15.1 Third party health service providers

The HPPs recognise that health service 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 of this manual).

The following guidelines are provided to assist health services to ensure privacy issues are addressed when disclosing personal health information to third party health service providers.

### 15.1.1 Informing patients

Admission and registration forms should include statements to the effect that:

- access to a client/patient's health record will be available to the client/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 client/patient's GPs and other providers involved in ongoing care with a discharge referral.

**Further guidance:**

- Section 7: Collecting personal health information.
- Appendix 5: Pro forma privacy leaflet for patients.

### 15.1.2 Health service provider obligations

Recognition that health service providers involved in ongoing care may access client/patient information is designed to enhance treatment provision by ensuring service providers have ready access to information relevant to care. In these circumstances however, health service 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 sort of information is made available. This is particularly likely to be the case in relation to personal health information collected for services such as sexual health, genetics, sexual assault, child protection. Health services should be aware of these concerns and endeavour to address them.

**Further guidance:**

- Refer to Section 15.9: Information specific laws and policies.

### 15.1.4 Conclusion of care

When an episode of care concludes for whatever reason (including the death of a client/patient), the right of access by a health care provider to the health record is normally terminated at the same time.

Access may still be authorised for purposes other than client/patient care, such as clinical audit or research, provided these fall within the HPPs.

### 15.1.5 Discharge referrals to GPs and others

It is standard practice to provide a client/patient's GP and other providers involved in ongoing care, (eg, community nursing, early childhood services) with a discharge summary.

Where GPs or other providers request access to the client\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 record, or the circumstances of the request must be fully documented on the client/patient's record.

**Further guidance:**

- Section 9.2.3.4: Electronic discharge referrals/summaries.

### 15.1.6 Records of a patient's family members

Requests by health care providers for access to the health records of members of a client/patient's family cannot be treated as exceptions to the rule and must be accompanied by the written consent of the person to whom the record relates (or an authorised representative).

## 15.2 Requests from State and Federal Police

### 15.2.1 Where disclosure to police is authorised by patient

Where a client/patient has authorised the police to have access to information from his/her records, this may be supplied on the standard police form P190 (ie expert certificate). If a police officer requests an expert certificate, refer them to the Health record Department, or facility equivalent, during office hours.

### 15.2.2 Where access is not authorised by patient

Section 11.2.7 provides detailed guidance on where the *HRIP Act* allows law enforcement agencies, including the NSW Police to access personal health information. These should be followed where the client/patient has not consented or has refused to release their information.

### 15.2.3 Search warrants

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 data.

### 15.2.4 Police interviews

#### 15.2.4.1 Interviews with clients/patients

Except in the case of declarations from dying client/patients, permission to interview a client/patient should only be given where the client/patient agrees and where the treating health service provider is of the opinion that the client/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 hand over times. The police visit should be documented in the health record.

#### 15.2.4.2 Interviews with clients/patients under the age of 16

If a client/patient is under the age of 16, a parent or legal guardian should be present during police questioning.

Alternatively, a parent or legal guardian can give permission for another person to be there.

If the client/patient is 16 or over, they can nominate an independent adult to be present during police questioning.

### 🕮 Further guidance:

- Child Protection Policy and Procedures Manual.

### ☎ Contact:

Child Protection & Violence Prevention Unit
NSW Department of Health
Tel. (02) 9424 5825

#### 15.2.4.3 Interviews with victims of sexual assault

Where police wish to interview the victim of a sexual assault, the relevant local Sexual Assault Service should be contacted.

#### 15.2.4.4 Interviews with staff

Where police wish to interview staff in relation to a matter that is unrelated to their work (eg, they may have witnessed a care accident or a crime), the health service will have no involvement in any interview, as it is purely a matter between staff member and police.

Where police seek to conduct an interview about an incident related to the health service (eg, in relation to a coronial matter or an assault on hospital premises) the staff member should be advised to contact their representative organisation, or a support person should be offered.

### 🕮 Further guidance:

- 11.2.3: To prevent a serious and imminent threat to health or welfare.
- 11.2.7: Law enforcement agencies, including police.
- 11.3.4: Reporting "serious criminal offences".

## 15.3 Child protection issues

NSW has a whole of government approach to child protection issues. Many information collection, sharing and disclosure issues are determined by either the *Children and Young Persons (Care and Protection) Act,* the NSW

Interagency Guidelines on Child Protection, or other NSW Health policy.

Common privacy issues affected by child protection rules are set out below. Key child protection policies are also set out at the end of this section, and staff are advised to refer to them to address detailed concerns in this area.

## 15.3.1 Reporting children at risk (Section 27)

Health workers are required to report to the Department of Community Services cases where they have "reasonable grounds to suspect that a child is at risk of harm". This obligation is imposed under Section 27 of the *Children and Young Persons (Care and Protection) Act.*

## 15.3.2 Information sharing with DoCS (Section 248)

Under Section 248 of the *Children and Young Persons (Care And Protection) Act,* DoCS can request a health service to provide information "relating to the safety, welfare and well-being of a particular child or young person or class of children or young persons".

DoCS and NSW Health have also developed detailed protocols for when and how Section 248 will be used.

## 15.3.3 Medical examinations (Section 173)

Under Section 173 of the *Children and Young Persons (Care And Protection) Act*, the Department of Community Services have the power to request a medical examination of a child.

When this occurs, any information obtained in the course of the examination may be disclosed to the Director-General of DoCS or a delegated officer, as the examination has been ordered under the authority of the *Act*. Information resulting from a medical examination can also be provided with consent of the parents or under Section 248.

## 15.3.4 Restrictions on access to child protection records

### 15.3.4.1 General rules

NSW Health has special policies for PANOC (Physical Abuse and Neglect of Children) Records. In accordance with these policies.

- PANOC records are generally held separately from the general health record.
- A register of children who have been seen via PANOC services has been established to allow:
  - linkage of the register to the general health record
  - alerts to be attached to the child's general health record where there is a serious and imminent threat to the life, health or safety of the child
  - additional restrictions to be placed on access by family members/parents where there is concern that access may place the child at risk (see Sections 11.3.2 and 15.3).

Records relating to child sexual assault are generally held by Sexual Assault Services, and will also be subject to these requirements.

### 15.3.4.2 Requests for information by parents

Where there is a request for access to a child's health record by a parent or guardian against whom an action in relation to child abuse may result, the treating health care provider may refuse access to that parent or guardian if it could be prejudicial to the physical or mental health of the child.

### 15.3.4.3 Staff safety

Child protection rules recognise that compliance with these obligations and support for child clients can place staff at risk. Due to this, the *Children and Young Person (Care and Protection) Act* provides that the names of staff who have made reports to DoCS are privileged and should not be disclosed.

**Further guidance** on Child Protection:

- PD2005_299: Protecting children and young people.
- Frontline Procedures for the Protection of Children and Young People (2000).
- NSW Interagency guidelines for child protection intervention.

All documents available at:
http://internal.health.nsw.gov.au/policy/hsp/child-protection.html.

**Contact:**

Child Protection & Violence Prevention Unit
NSW Department of Health
Tel. (02) 9424 5825

**Further guidance** on Staff Safety:

- PD2005_315: Zero Tolerance: Response to violence in NSW Health workplace.

**Contact:**

Employee Relations Unit
NSW Department of Health
Tel. (02) 9391 9305

## 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.

## 15.5 Use of interpreters

Clients/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.

Professional interpreters should be made available and the decision to use an interpreter should rest with the client/patient. This is particularly important where the information to be discussed is complex, likely to be considered sensitive by the client/patient or where the client/patient may be at risk of harm, for example, if they are victim to domestic violence or sexual assault. The gender of the interpreter should also be taken into consideration.

Health service providers may need to request the services of an interpreter if they have difficulty understanding a client/patient or are unsure about whether the client/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 client/patient and obtain informed consent if appropriate.

Where adapting the pro forma privacy leaflet for patients (see 7.4.5) for more specialised services, consideration should also be given to translation of the revised leaflet.

Interpreters are obliged to keep confidential any personal information they may access in the course of their duties.

**Further guidance:**

- PD2005_281: Standard procedures for the use of health care interpreters.
- PD2005_413: Identifying & responding to domestic violence.

## 15.6 Legal claims and insurance

### 15.6.1 Claims manager and treasury managed fund

Cooperation is to be afforded where the health service's public liability insurer is the Government Insurance Office (GIO). Access to personal health information which is relevant to the claim may be provided to the solicitor for the GIO when acting on behalf of a defendant health service in cases covered by the Master Public Liability Insurance Policy (Treasury Managed Fund).

Such access does not require authorisation from the client/patient. The senior health care provider should be informed of such requests.

### 15.6.2 Client/patient's legal representative

Where the client/patient's legal representative has been authorised to view the complete health record of a client/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 PD2005_235: Charges for Health Records & Medical Reports.

### 15.6.3 Client/patient's insurer

Where a request is made for information related to an insurance, compensation or workers compensation claim, a photocopy of the insurance application or compensation claim form. The claim/application form should be signed and dated by the client/patient, containing the client/patient's consent to disclosure, is sufficient authority for the release of a medical report or summary of injuries.

Other information should not be provided without the clearly documented consent of the client/patient.

### 📖 Further guidance:

- PD2005_235: Charges for Health Records & Medical Reports.

## 15.7 Media and other enquiries about hospital patients

### 15.7.1 Enquiries about clients/patients

A health service may neither confirm nor deny the current or past presence of a person, unless the enquirer already knows that the client/patient is present.

Where staff are satisfied the enquirer knows the client/patient is present they may indicate ward details provided they believe that to do so would not be contrary to the interests of the client/patient. If in doubt, or where there is a record of domestic violence, the client/patient should be consulted prior to details being provided to a third party.

Where a client/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 client/patient lists used by the enquiry section may be modified accordingly.

### 15.7.2 Other safeguards for enquiries sections

Health services should ensure that client/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 (eg Ward A instead of psychiatric ward, colorectal unit etc).

### 15.7.3 Media queries

No information about a client/patient should be released to the media without the consent of that client/patient. In addition, if the request includes requests for clinical or other information, these should be referred to the senior health care provider.

If the client/patient is conscious and can communicate, he/she should be asked whether information may be given. If the client/patient is deceased or is not conscious, the "authorised representative" (see 5.5) must be asked before information is given.

Any decision to disclose material held on a deceased client/patient should also have due regard to any view expressed by the client/patient to health workers prior to death, either in writing, or as recorded in the client/patient's health record.

#### 15.7.3.1 Responsibility for media liaison

All media inquiries should be directed to Health Public Affairs Media Issues Management. A designated media liaison or public affairs officer should always be the first point of contact for the media. A media liaison officer from the Department is available at all times via the on call 24-hour media pager. Every area health service also has an on call media liaison officer.

#### 15.7.3.2 Accident victims

Information released about accident victims should be limited to the number of casualties, sex, approximate age and whether injuries are critical, serious or minor.

#### 15.7.3.3 Information about medical practitioners

Medical news regarding a client/patient should not refer to a medical practitioner in private practice.

If information is released to the media an assurance should be sought from the facility concerned that the name of the client/patients treating medical practitioner will not be published.

#### 15.7.3.4 Tapes or images of clients/patients

A client/patient should not be photographed, or recorded on videotape or audiotape outside clinical/care requirements unless:

- the client/patient requests this or agrees in writing
- the opinion of the treating health care provider is that the client/patient's condition will not be jeopardised.

The client/patient should be informed about the purpose of the tape or image eg therapy, health promotion, publicity etc.

## 15.8 Fundraising

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 client/patient at the time of collection of that information.

The form of the consent request should be approved by the relevant Human Research Ethics Committee (HREC). The right to withhold consent should be made clear at the time such consent is sought.

Clients/patients have a right to withdraw consent and to have their names and addresses removed from any lists held. To this end:

- direct mail should contain a statement of the addressee's right to have his/her name removed from mailing lists
- correspondence should clearly display the name and full address of the sender.

Committees involved in fundraising and/or public support campaigns should ensure that names and addresses are deleted from mailing lists promptly when requested.

### 15.8.1 Limits on what information may be used

The information which may be released with consent is limited to name and address. Information relating in any way to a client/patient's health status is not to be included in information made accessible for fundraising and public support campaigns.

### 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 9.1).

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 or any personal health information held by that committee once they have ceased to be a member of the committee.

Committees are not to release to or exchange with any third party, lists containing personal health information.

### 15.8.3 Organisations with a commercial interest

Information regarding clients/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, dealing as it does with matters that are extremely personal and which a client/patient will generally expect to be shielded from public disclosure. The terms of the *HRIP Act* are based on adopting and reflecting these expectations.

As noted in 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 NSW Department of Health and the Aboriginal Health and Medical Research Council (AHMRC), the peak body representing Aboriginal Community Controlled Medical Services in NSW, have developed the Aboriginal Health Information Guidelines (AHIG). These guidelines provide a framework of ethical and culturally sensitive protocols for the collection and use of personal health information relating to Aboriginal and Torres Strait Islander peoples in New South Wales.

Requests for access to Aboriginal health information and the collection of information (including personal health information) from Aboriginal communities must demonstrate compliance with the terms of the AHIG, and information users must agree in writing to adhere to its terms. It is recommended that such requests should be referred to the Centre for Health for consideration and advice.

### 🕮 Further guidance:

- NSW Aboriginal Health Information Guidelines.

### ☎ Contact:

Centre for Aboriginal Health
NSW Department of Health
Tel. (02) 9391 9502

## 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 Family Information Service of the Department of Community Services. See the Patient Matters Manual Section 9 for full procedures.

Provided the identity (or information that may assist in identification) of the biological parents is withheld, information from the health record may be released on receipt of an authorised request from the Department of Community Services.

Where a request is received from a person or organisation other than the Department of Community Services, the facility should contact that Department 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 records, copies of correspondence should be kept physically separate from the biological parents' records.

## 15.9.3 Service based policies

### 15.9.3.1 Genetics services

Information collected by a NSW Genetics Service often includes an extensive family tree with information about the health status of other relatives without their knowledge or permission. Specialised genetics records should be stored securely and preferably separately. Genetic health records should be held indefinitely due to the potential value of family health tree information to other family members, particularly in following generations.

#### Third party access – insurers and employers

The results of predictive or presymptomatic 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, client/patient consent must be sought prior to disclosure. There is no obligation on a health service provider to disclose information to such a third party.

#### Third party access – family members

When disclosure of genetic information would allow early detection or effective treatment of a condition or affect important life decisions for other family members, the client/patient's rights under privacy law do not change. Disclosure of the genetic information in order to provide care or treatment to another person, even a family member is not a "directly related purpose". As a result, client/patient consent is required prior to the disclosure of personal genetics information to a blood relative or for purposes relating to a blood relative's health care.

Where a health care provider anticipates a situation where information will be obtained from a client/patient which may be of interest or potential benefit to other family members, he or she should discuss this with the client/patient prior to treatment being commenced or as part of protocols for ordering tests. Through counseling, individuals should be encouraged to accept their own responsibilities with regard to the information needs and rights of others.

### 🕮 Further guidance:

- NSW Health Ethical Code Governing the Provision of Genetics Services.
- NHMRC Guidelines for the Use of Genetic Registers in Medical Research.

### 15.9.3.2 Child protection services

The specific policies and laws relating to access and disclosure of child protection information and records are set out in Section 15.3, which provides more detailed guidance on child protection service issues.

### 15.9.3.3 Sexual Assault Services

NSW Health has special policies for management of information collected by NSW Sexual Assault Services. In accordance with these policies:

- files are generally maintained separately
- files can be linked to the general health record only via a notation that a "confidential file 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 Sexual Assault Service, who in turn will seek client consent.

### 🕮 Further guidance:

- NSW Health Sexual Assault Services Policy and Procedures Manual 1999.

## 15.9.4 Service based practices

There is no overarching NSW Health Policy dealing with how the personal information collected by stand alone drug and alcohol or sexual health services should be managed. Recognising however that clients attending these type of stand alone services will often have expectations about how their information has been used, these Services tended, as a matter of practice, to develop specific practices in management of the personal information they collect.

### 15.9.4.1 Drug and alcohol services

Drug and alcohol services are often provided from stand alone services, not integrated into a general hospital. As such, clients may have more limited expectations as to when and how their information will be shared. Health records of these services are also often held separately from any general health record.

As at June 2005, NSW Health is in the process of developing a revised privacy leaflet for patients for drug and alcohol services which will provide more specific information about what clients of these services can expect. The leaflet will indicate that while records will continue to be kept separately, information necessary for ongoing care and treatment for other medical conditions will be made available on request. Where a client/patient raises concerns about such sharing of information, the service will seek to accommodate these concerns, as outlined in Section 11.2.1.3 Outside client/patient's "reasonable expectation".

### ☎ Contact:

Centre for Drug and Alcohol
NSW Department of Health
Tel. (02) 9391 9262

### 15.9.4.2 Sexual health services

Sexual health services are often provided from stand alone services, not integrated into a general hospital. Health records of these services are usually held separately from any general health record. As such, clients may have different expectations as to when and how their information will be shared. Most sexual health services have policies which rely on extensive client/patient consents to determine how and when information about the services received by a client can be disclosed.

In addition, the *HRIP Act* 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 persons HIV status under the *Public Health Act.*

### 🕮 Further guidance:

- Section 4.1.3: Public Health Act.
- Section 11: Using and disclosing personal health information.
- Section 15.9.5: Managing Public Health Risks.
- PD2005_134: HIV Confidentiality: A Guide to Legal Requirements.

## 15.9.5 Organ and tissue donor information

In order 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 or 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
- in connection with the administration or execution of the *Human Tissue Act*
- 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:

- PD2005_341: Use and Retention of Human Tissue including Organ Donation, Post Mortem Examination and Coronial Matters.

### 15.9.6 Managing public health risks

The *Public Health Act* establishes a range of provisions which impact on the management of personal health information. The main intent of these provisions is to ensure there are appropriate powers available to the Director-General to take action when a matter involving risk to public health arises (such as for example outbreaks of food poisoning or disease).

#### Reporting of certain medical conditions and diseases

The *Public Health Act* also establishes requirements for doctors, hospital chief executive officers and laboratories to notify certain diseases to Public Health Units.

### 📖 Further guidance:

- PD2005_359: Notification of Infectious Diseases under the Public Health Act 1991.

#### ☎ Contact tracing

NSW Health has policies in place providing for contact tracing based on a number of factors including consideration of the risk exposure and the nature of the disease.

Contact tracing is generally undertaken with the consent of the index client/patient. Contact tracing without index client/patient consent cannot occur unless it has been given prior authorisation by the Director-General, NSW Department of Health. The parameters for non-consensual contact tracing are established by clause 10 of the Public Health Regulation. Under this clause, the Director-General or a delegate, 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 (eg diagnosis, treatment and prevention) to prevent further transmission of infection.

Clause 10 does not permit the disclosure of the name of the index case so health care workers must be careful not to reveal the identity of the index case. If the identity of the index case is obvious to the person being notified, then this is regarded as an unavoidable consequence of the contact tracing and the health care worker involved would not be in breach of the statutory client/patient privacy or confidentiality provisions.

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:

- PD2005_184: Contact tracing guidelines for the sexually transmissible diseases and blood borne viruses.
- PD2005_258: Management of people with HIV infection who risk infecting others.
- PD2005_194: HIV Antibody Testing by Laboratories in NSW.
- Commonwealth Department of Health and Family Services National Contact Tracing Manual.

### ☎ Contact:

For further assistance contact the local area health service specialist sexual health service or Public Health Unit.

#### Undertaking public health inquiries

Section 71 of the *Public Health Act* gives the Director-General broad powers to inquire into any matter relating to the health of the public. A person authorised by the Director-General for the purposes of such an inquiry is entitled to enter premises inspect and copy records. These powers can only be exercised however where the person has been issued with a Certificate of Authority by the Director-General under Section 72 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 11.2.9)
- provisions allowing an authorised representative to make a decision on behalf of a person (see 5.5)

- other grounds allowing use or access provided for under HPPs 10 and 11
- provisions relating to access to information held by a health service provided for under the *Freedom of Information Act.*

Any decision to disclose material held on a deceased client/patient should also have due regard to any view expressed by the client/patient prior to death, either in writing, or as recorded on the client/patient's medical file. This would include any "advanced directive" made by the client/patient.

## 15.11 Telehealth

The primary objective of telehealth is to enhance access to and equity of health services and resources for residents of both metropolitan and country areas of New South Wales by enabling real time, remote clinical consultation and more efficient transmission, storage and sharing of client/patient information. Specific privacy issues arise from the use of image transfer and clinical consultations conducted by videoconference. The protocols issued by the NSW Telehealth Program include guidance on how to address the specific privacy issues which arise in this type of service provision.

## 15.12 Community health records

### 15.12.1 Group houses/hostels

Comprehensive health records of clients/patients residing in ward-in-a-house, group houses or hostels should continue to be maintained and stored at the nearest community health facility.

The non-institutional nature of group houses and hostels may pose particular threats to the confidentiality of personal health information and special precautions should be taken to ensure that client/patient privacy is maintained.

Records should be stored in a secure place, inaccessible to clients and visitors. 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
- day book
- card index or mini-file: should include identification data, referral information and medication details.

### 15.12.2 Group sessions

Individual client/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 client/patient.

### 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 client/patient. Extreme care should be taken to safeguard the privacy of other family members.

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 client/patient is released.

### 📖 Further guidance:

- 15.9.3.1 Genetics services.

## 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 *HRIP Act* 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. See Appendix 4.3 for a sample privacy notice.

### 15.13.1 Quality of health records

The health record should comply with Section 9 and be sufficiently detailed and comprehensive to:

- provide effective communication to health care providers
- provide for a client/patient's effective, ongoing care
- enable evaluation of the client/patient's progress and health outcome
- retain its integrity over time.

Because the primary purpose of keeping health records is to enable better client/patient care, it is important that the information in the 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 health care provider their designation, the date and time clearly legible
- 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 care provider should periodically review the record for correctness
- there should be an audit trail for electronic records.

For detailed procedures regarding accuracy and completeness of health records see Section 9 of the Patient Matters Manual.

### 15.13.3 Control of health records

Control over the movement of records is of the up most importance. An adequate record tracking system, tailored to local needs, is essential to facilitate prompt record location and ensure that client/patient care does not suffer and that privacy is not breached.

Systems for transporting health records within a health service should be well supervised to ensure that the records are not accessible by unauthorised persons. No document from a health record should be removed from that record without being replaced by a tracer note. The tracer should specify document destination and date document was removed. The tracer should remain on the health record until the document is returned.

No health record should be removed from its home location (ie the Medical Record Department) without the following details being recorded in an appropriate system:

- medical record number
- client/patient name
- destination/location of the health record
- person responsible for/in possession of the health record
- date health record was removed.

Records subject to the Sexual Assault Communications Privilege should be marked confidential and transported in sealed envelopes.

### 15.13.4 Removal

Records should be kept under adequate security as outlined in Section 9 and the original only removed from the health service upon a court subpoena, statutory authority, search warrant, coronial summons (see Section 9 of the Patient Matters Manual) or order of the Director-General, NSW Department of Health.

Whenever the original of a major health record leaves a health service, a copy of that record should, where possible, be made beforehand and kept.

### 15.13.5 Transfer

It is the responsibility of th estaff member who receives the record to ensure it is kept in a secure location to prevent loss and unauthorised access.

### 15.13.6 Storage, archiving and disposal

Record disposal should comply with Section 9.1 and take into account the type of information contained in a record and possible future demand for it as well as the needs of individual health services. In particular the following should be considered:

- use of records for client/patient care, medico-legal purposes and research and teaching
- archival value
- provisions of the *Evidence Act 1995* and the Statute of Limitations
- available storage space
- requirements under the provisions of the *State Records Act 1998.*

Similar standards for maintaining privacy and security should be maintained for records in archival or secondary storage as for records in current use.

### 📖 Further guidance:

- General Disposal Authority (GDA17) Public health services: Patient/Client Records (State Records NSW) www.records.nsw.gov.au.

### 15.13.7 Health facility closures

When a facility is closed, each responsible unit should create a file that includes details of:

- records or documents destroyed
- documents retained
- documents transferred to other locations
- officers who undertook closures.

## 15.14 NSW data collections

### 15.14.1 NSW Health data

Statistical information and other data are submitted to the Department 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 1991*, the *Health Administration Act 1982*, and the *Private Hospitals and Day Procedure Centres Act 1988*.

The framework for collection and use of data is set out in the NSW Health Information Policy, available at: http://internal.health.nsw.gov.au/im/ims/di/information-policies-and-strategies.html

### 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 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.

### 📖 Further guidance:

- Health Information Resources Directory.
- http://internal4.health.nsw.gov.au/hird/index.cfm.
- Information Management Guideline: Staff Roles and Responsibilities.
- http://internal.health.nsw.gov.au/im/ims/di/information-policies-and-strategies.html.

## 15.14.4 Access to data collections

Where data collections contain identifying or potentially identifying information, HPP 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 11.1)
- the access is for a directly related purpose, which would be "reasonably expected" by the individual (see 11.2.1)
- the access is required or authorised by law (see 11.3)
- use or disclosure for management or research purposes (see 11.2.4).

Where access is sought for research or management purposes, the NSW Privacy Commissioner's Statutory Guidelines on Research and the Statutory Guidelines on Management. 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 Department of Health, applications should be made to the NSW Department of Health Ethics Committee (DOHEC).

Based on the evaluation report of the HREC or the DOHEC, 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 restraints applying.

### 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 *HRIP Act*, and to abide by any other conditions or constraints (relating to charges, monitoring requirements etc) on the use of the data set by the data custodian.

Although NSW Health will endeavour 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.

Access, when granted, will 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 will 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.

### 15.14.4.2 Records linkage

Linkage of specific data is authorised under the *HRIP Act* provided the linkage is necessary for the purposes of management or research and the Statutory Guidelines have been complied with.

Linkage of whole health records for the purposes of establishing an ongoing health care record must, however, comply with HPP 15.

### 15.14.4.3 NSW Department of Health Ethics Committee (DOHEC)

The DOHEC 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 DOHEC also considers:

- proposals for data use or issues requiring ethical advice referred by NSW Department of Health officers
- multi-centre research proposals
- proposals referred by HRECs
- proposals for data linking.

# Electronic health records 16

Electronic records differ from paper records in ways that warrant special consideration. Firstly, it is possible to have a single electronic record simultaneously accessible at multiple sites, giving more people access. Secondly, it is possible to control access to an electronic record in ways that are not possible with a paper record.

As at June 2005, the NSW Department of Health was in the process of developing formal policy to provide practical solutions to privacy and security issues.

The principles set out below are primarily for guidance and support, and will operate subject to those policies once issued.

## 16.1 Fundamental principles

The *HRIP Act* requires that health service staff only access personal health information when it is necessary for them to do so to carry out their role in providing health services. Electronic systems facilitate access to information. Given this, staff and provider awareness of their obligation to restrict access to what is clinically necessary or otherwise authorised under the law becomes more critical. Systems to audit and ensure compliance with these obligations also become critical.

The following principles have been developed by the NSW Department of Health Electronic Medical Record (eMR) team in consultation with health service staff involved in the implementation of the eMR, and health service privacy contact officers. The principles are fundamental to ensuring that staff are made aware of their duties of confidentiality when accessing electronic health records:

1. **Privacy and confidentiality undertakings for staff**: Staff must sign a privacy undertaking on employment (see Appendix 3.2) outlining their responsibility to observe the Health Privacy Principles and duties of confidentiality.
2. **Training and informing staff**: Health service staff must be able to access and use electronic records properly. Appropriate education and training should be provided.

   Staff must also be informed and regularly reminded of their responsibilities to client/patient privacy and confidentiality. On one level this can be achieved through a combination of staff induction, staff meetings, training, staff newsletters, notices, posters, and so on. Informing staff should also be achieved by building alerts and notifications into the electronic systems, in particular with categories of personal health information collected by specialist services (see 15.9).
3. **Auditing**: Access to personal health information should be audited on an ongoing basis, with the possibility of reports and notifications being generated regarding access to records. Systems must be in place to appropriately manage breaches of access.
4. **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 pro forma privacy leaflet for patients (see Appendix 5).

## 16.2 *Evidence Act*

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 also need to be implemented to ensure that images cannot be altered between scanning and storage or while stored.

## 16.3 Accountability

Information technology staff need to have some form of control over electronic records. Implementation of access rules and some degree of control will pass from health care providers and health information managers to system staff (see 16.1). To ensure the integrity of electronic records there is a need to specify accountability for the system which delivers the record and for its processing. Failsafe backup will be required in case of disaster.

Whoever enters the information into the health care record, is accountable both for the quality of that record and the care that has been documented.

## 16.4 Access and quality control

The area over which the electronic record is available is significant, ie individual facility, campus or area health service. The broader the system, the tighter the network and access controls will be needed.

Individual user names and passwords should be used rather than generic ones for staff category.

Where the electronic record system covers multiple facilities, the records may contain a mix of entries from different sources or partial copies of records from other facilities. The ability to maintain a single, logical record in this situation is critical. This can be achieved through various means such as appropriate labelling of each transaction and adequate version control. Identification and authentication of the person making the entry is important.

Electronic records should meet the same quality criteria as paper records. When amendments are made to clinical information the original data should be retained.

## 16.5 Patient access

It is important to ensure that the right of client/patients to access their own records is not compromised by the introduction of electronic records and resulting changes in retention and storage procedures. Adequate viewing and copying facilities should be readily available.

### 🕮 Further guidance:

- refer to specific electronic health records policies, available at: http://internal.health.nsw.gov.au/im/.
- http://internal.health.nsw.gov.au/im/ibs/ehr.
- http://internal.health.nsw.gov.au:2001/emr.

# Appendix 1: List of relevant policies

## A.1.1 NSW Policy directives

**Available at:**
**www.health.nsw.gov.au/policies/index.htm**

Chaplaincy Services and Privacy Law (PD2005_412).

Chaplaincy Services to the NSW public health system (PD2005_123).

Charges for Health Records and Medical Reports (PD2005_235).

Contact Tracing Guidelines for Sexually Transmissible Diseases and Blood Borne Viruses (PD2005_184).

*Coroners' Cases and Amendments to Coroners Act 1980* (PD2005_352).

Electronic Information Security Policy (PD2005_314).

HIV Confidentiality: A Guide to Legal Requirements (PD2005_134).

Identifying and responding to domestic violence (PD2005_413).

Patient Information and Consent to Medical Treatment (PD2005_406).

Privacy Management Plan and Internal Review Guidelines (PD2005_554).

Principles and Minimum Standards for the development of health services codes of conduct (PD2005_130).

Principles for Creation, Management, Storage and Disposal of Health Care Records. (PD2005_127).

Process for Approval of New or Modified data collections (PD2005_155).

Protecting Children and Young People (PD2005_299).

Protecting People and Property: NSW Health Policy and Guidelines for Security Risk Management in Health Facilities (PD2005_339).

Standard procedures for the use of health care interpreters (PD2005_281).

Subpoenas (PD2005_405).

Use and Retention of Human Tissue including Organ Donation, Post Mortem Examination and Coronial Matters (PD2005_341).

Workplace Health and Safety: Policy and Better Practice Guide (PD2005_409).

Zero Tolerance: Response to violence in NSW Health workplace (PD2005_315).

## A.1.2 Other NSW Health policies

Child Protection Policy and Procedures Manual.

Frontline Procedures for the Protection of Children and Young People (2000).

Interagency Guidelines for Child Protection Intervention.

Sexual Assault Services Policy and Procedure Manual.

## A.1.3 Other government policies

NSW Premiers Circular No. 2001–46.

NSW Premiers Circular No. 2004–06.

General Disposal Authority (GDA 17) Public health services: Patient/Client Records.

Australian Standard for electronic systems AS7799.

# Appendix 2: List of relevant laws

**Note**: The *Health Records and Information Privacy Act 2002* (*HRIP Act*) is relevant throughout the Privacy Manual and is therefore not listed here.

| Acts referred to in Privacy Manual | Privacy Manual Reference |
|---|---|
| *Children and Young Persons (Care and Protection) Act 1998* | Section 11.3.2, Section 15.3 |
| *Commission for Children and Young People Act 1998* | Section 11.3.10 |
| *Coroner's Act 1980* | Section 11.3.5 |
| *Crimes Act 1900* | Section 11.3.4 |
| *Evidence Act 1995* | Section 11.2.2, Section 12.5, Section 15.13.6, Section 16.2 |
| *Freedom of Information Act 1989* | Section 4.2, Section 12.2, Section 15.10 |
| *Guardianship Act 1987* | Section 5.6 |
| *Health Administration Act 1982* | Section 4.1, Section 15.14.1 |
| *Health Care Complaints Act 1993* | Section 15.9.4 |
| *Health Services Act* 1997 | Section 7.1, Section 11.3.1, Section 11.3.13 |
| *Human Tissue Act 1983* | Section 15.9.4 |
| *Migration Act 1958* (Cth) | Section 11.3.12.3 |
| *Mental Health Act 1990* | Section 4.1.2, Section 11.3.9 |
| *Occupational Health and Safety Act 2000* | Section 11.3.11 |
| *Ombudsman's Act 1974* | Section 11.3.8, |
| *Public Health Act 1991* | Section 4.1.1, Section 4.1.3, Section 8.2, Section 11.2.3.3, Section 11.3.13, Section 15.9.3, Section 15.9.5, Section 15.14.1 |
| *Privacy and Personal Information Protection Act 1998* | Section 2, Section 4.1, Section 6.5, Section 14 |
| *Privacy Act 1988* (Cth) | Section 4.1.4, Section 13.2.1 |
| *Private Hospitals and Day Procedure Centres Act 1988* | Section 11.3.1, Section 11.3.13, Section 15.14.1 |
| *Registration of Births, Deaths and Marriages (Amendment) Act 1973* | Section 11.3.13 |
| *Social Security (Administration) Act 1999* (Cth) | Section 11.3.12.1 |
| *State Records Act 1998* | Section 4.2, Section 9.1, Section 15.13.6 |
| *Veterans' Entitlement Act 1986* (Cth) | Section 8.2, Section 11.3.12.2 |

# Appendix 3: Pro forma privacy undertaking

(**Reference** Section 9)

## A.3.1 Privacy undertaking (general)

I, (name).....understand that, while I am (employed/contracted*) by the (name of health service), I may have access to personal health information collected for purposes of client/patient care or for administrative, statistical or other purposes. Such personal information includes the identity of, and personal and health information about individual persons.

I undertake not to knowingly access any personal health information unless such information is essential for me to properly and efficiently perform my (duties/contractual obligations*).

I recognise and accept that my access to, holding and use of this information is subject to the Health Privacy Principles contained in the *Health Records and Information Privacy Act 2002* (copy of Health Privacy Principles attached) and undertake to comply with those Principles and relevant NSW Health Policies affecting the collection, holding, use or disclosure of the information.

In order to fulfill this undertaking, I will not divulge any personal health information regarding individual persons, except as allowed by the Health Privacy Principles.

I also undertake to follow other information privacy and security procedures as stipulated by NSW Health Policies in relation to any personal health information which I access in the course of my (duties/contractual obligations*).

In order to fulfill this undertaking I will ensure that, so far as is within my control, such information, whether in the form of paper documents, computerised data or in any other form, cannot be viewed by unauthorised persons, and that the information is stored in a secure and orderly manner which prevents unauthorised access.

I further undertake to inform (my supervisor/title of relevant officer*) immediately if I become aware of any breach of privacy or security relating to the information which I access in the course of my (duties/contractual obligations*).

| | |
|---|---|
| Signed..... | Witnessed..... |
| .....<br>(name) | .....<br>(name) |
| .....<br>(signature) | .....<br>(signature) |
| .....<br>(position) | .....<br>( position) |
| (date) | (date) |

* delete as required

(**Reference** Section 16.1)

## A.3.2 Electronic medical record privacy undertaking

I, .....……..... (name), understand that while I am employed by the .....……..... (name of health service) I will have access to personal health information collected from patients that is protected by privacy law. I undertake not to knowingly access any personal information, such as information contained in a client/patient's medical record and in the electronic medical record (eMR) system, unless such information is essential for me to properly and efficiently perform my duties.

I recognise and accept that my access to, holding and use of this information is subject to the Health Privacy Principles contained in the *NSW Health Records and Information Privacy Act 2002* (copy of Health Privacy Principles attached). In order to fulfil this undertaking, I will not divulge any personal information regarding individual persons, except as allowed by the Health Privacy Principles.

I undertake to comply with other information privacy and security procedures as stipulated by NSW Health policies* in relation to any personal information that I access in the course of my duties. In order to fulfil this undertaking I will ensure that, so far as is within my control, such information, whether in the form of paper documents, computerised data or in any other form, cannot be viewed by unauthorised persons, and that the information is stored in a secure and orderly manner that prevents unauthorised access.

I further undertake to inform (my supervisor/title of relevant officer) immediately if I become aware of any breach of privacy or security relating to the information that I access in the course of my duties.

| | |
|---|---|
| Signed..... | Witnessed..... |
| .....<br>(name) | .....<br>(name) |
| .....<br>(signature) | .....<br>(signature) |
| .....<br>(position) | .....<br>( position) |
| (date) | (date) |

* Relevant NSW Health policy directives include:

- PD2005_362: NSW Health Privacy Manual.
- PD2005_314: Electronic Information Security Policy.
- PD2005_155: Process for Approval of New or Modified Data Collections.

## A.3.3 Contractual provisions

The types of provisions which should be included where data is transferred to an external contractor for work include:

**Acknowledgement of privacy laws**

- **Recognize** that the information must be handled in accordance with relevant privacy laws.

**Purpose**

- Clearly **define the purpose** for which it will be used and the disclosures (if any) allowable under the contract.
- Require the contractor **not to use or disclose** the information for any other purpose without appropriate written consent of the health service.
- **Require the data to be destroyed** or returned to the health service after use or at the termination/completion of the contract.

**Security**

- Information provided must be handled in a **secure manner**.
- The **contractor is responsible** for ensuring the appropriate security for and disposal of the information.
- **No copies** to be made of the information unless the copies are reasonably necessary for the defined purpose or made with the written permission of the health service.
- Contractor must ensure that all information sent to it under the contract via disc, ftp, email, gopher, Internet or other media is **moved to a secure computer storage** as soon as received.
- The contractor to **ensure information is disclosed to as few persons** within its organisation as are reasonably necessary for the defined purposes for which the information was supplied.

# Appendix 4: Pro forma privacy notices

## A.4.1 Fax cover sheet

(**Reference** Section 9.2.3.2.)

**Privacy notice:**

The information contained in this fax message is intended for the named addressee only. If you are not the intended recipient you must not copy, distribute, take any action reliant on, or disclose any details of the information in this fax to any other person or organisation. If you have received this fax in error please notify us immediately.

## A.4.2 Patient charts/end of patient bed

(**Reference** Section 9.2.1)

**Privacy notice:**

Information contained in patient charts is protected by privacy law, and must only be accessed by health workers directly involved in the patient's care. Relatives and visitors must not access patient charts, unless they have received consent from the patient to do so.

## A.4.3 Health records

(**Reference** Section 15.13)

**Privacy notice:**

The information contained in this record is protected by law from unauthorised access and misuse. The information must only be accessed by health workers directly involved in the patient's care, or with other lawful excuse. For further information refer to the NSW Health Privacy Manual.

# Appendix 5: Pro forma Privacy leaflet for patients

(**Reference** Section 7.4)

**The pro forma privacy leaflet for patients is to be adapted by health services for distribution to patients. *See Section 7.4 of the manual for further guidance.* A soft copy of the leaflet is available from the privacy intranet page, or by emailing: privacy@doh.health.nsw.gov.au**

**Proforma**

to be adapted by health services for distribution to patients.

**(Name of Health service)**

**Privacy leaflet for patients**

### Our obligations

The NSW public health service is committed to safeguarding the privacy of patient information, and has implemented measures to comply with its obligations under the Health Records and Information Privacy Act 2002. All staff are bound by the Act and by NSW Health privacy policy.

This leaflet provides you with details of what personal information is held about you, how you can access this information and the purposes for which your personal information is used and disclosed. Your personal information includes your personal details and personal health information relating to your treatment.

### Collection

We collect your personal information so that we can provide you with treatment and medical advice. Test results and further information collected while you are being treated are kept with your health record. We collect information that is relevant and necessary for your treatment and to manage the health service.

We collect information directly from you, wherever possible. We may need to collect information from other health professionals who have treated you. In an emergency we may also need to collect information from a family member, friend, carer or other person who can help us to provide you with the best care.

Your information may be held in paper and electronic files. We take all reasonable steps to ensure the information we collect about you is stored securely. We are required by law to retain health records for certain periods of time depending on the type of record and facility. We have appropriate systems and policies in place to protect your information from loss, unauthorised access and misuse.

If you do not wish for us to collect certain information about you, you need to tell us and we will discuss with you any consequences this may have for your health care.

### Use and disclosure

All staff are bound by law and ethical practice to keep your information confidential. Staff will use or disclose your information for purposes directly related to your treatment, and in ways that you would reasonably expect for your current and future care.

Your personal health information will be shared with staff involved in your care in order to determine the best treatment for you and to assist in the management of the health services provided to you.

Relevant information about the health services you have received will be sent to your nominated GP, unless you request otherwise. Where relevant, information will be sent to other treating health services or hospitals involved in your care, or to the Ambulance Service of NSW, to a specialist for a referral, for pathology tests, x-rays, and so on.

We may be required to disclose some patient information to Courts and Tribunals and to State and Commonwealth government agencies to comply with other laws, for example to report notifiable diseases, provide statistics, and for the registering of births & deaths. Your personal information may be required as evidence in court if subpoenaed.

We may use or disclose patient information for billing and other purposes required for the operation of the NSW health service, including safety and quality improvement initiatives. Where relevant, we may need to disclose patient information to Medicare, private health funds, the Department of Veterans' Affairs, The Australian Council on Healthcare Standards (or similar accreditation body).

We may use your information to contact you regarding patient satisfaction surveys that help us to evaluate and improve our services.

We may use or disclose your information for the following purposes in accordance with Statutory Guidelines issued under privacy law for:

- public interest research projects complying with strict protocols and approved by a Human Research & Ethics Committee
- staff and student training purposes
- other planning, financial or management purposes for health service activities.

The Statutory Guidelines ensure that where your information is needed for these purposes and it is impracticable to seek your consent, a minimum amount of personal information is used, and the personal information is handled in accordance with strict standards.

We will seek your consent prior to the use or disclosure of patient information for purposes other than those listed above, such as for fundraising activities.

### Access to your information

You are entitled to request access to all personal information including your health record held by health service providers in NSW. Normally you will be asked to apply for access in writing and provide identification. You may be charged a fee if you request copies of your personal information or health record.

Access to your personal information may be declined in special circumstances, such as where giving access would put you or another person at risk of harm.

If you believe the information we hold about you is incorrect and an error has been made, please let us know and we will correct the information. If we believe the information is correct, you may request for your view to be noted on the record.

Requests for access to or correction of your health record should be addressed either to the Medical Record Department or the General Manager of the health service facility you attended.

### ☎ Contact us

If you have questions or a complaint about the privacy of your personal information, please contact (AHS Contact details) or (AHS stamp).

# Index

## A


Aboriginal health information.....51-52
access to records by patients.....**41-42**, *see also* records
accident victims, information about.....50
accountability, in electronic records.....60
accuracy of records.....7, **26**, 56
acronyms.....**1-2**
additions to records, see amendments to records
Administrative Decisions Tribunal, complaint handling procedures.....45
admission forms .....46
adoption information .....52
AIDS, see HIV-related information
alcohol and drug services.....53
alterations to records, see amendments to records
Ambulance Service of New South Wales.....4
amendments to records .....**41-42**, *see also* records
anonymity rights of patients/clients.....22
archiving of records.....56-57
audiotape of patients/clients.....50
auditors, disclosure to.....28, 59
Australia, transferring information out of .....43-44
authorised representatives.....14-15, 49


## C


capacity to give consent .....13
capacity to understand .....19
charges for information access .....30, 42
chief executives .....16
Chief Health Officer, may release epidemiological data 8
children, see also Department of Community Services (NSW); parents and guardians at risk of violence....37
capacity to give consent.....14
Child Death Review Team.....39
child protection issues.....48-49, 52
health examinations at school .....48
information requests from parents .....41
interviews with police.....47
perinatal deaths, obligation to report .....40
*Children and Young Persons Care and Protection Act 1998* (Cth) .....37,48
claims managers.....49
clients, see patients/clients
clinical placements.....33
codes of conduct.....10
collection principles.....**18-21**, *see also* records
commercial interests, see non-government organisations
*Commission for Children and Young People Act 1998:* .. .....39
common law .....10
Commonwealth Agencies, powers of.....39-40
*Commonwealth Privacy Act 1988*:.....9
community health records .....55
Community Services Department, see Department of Community Services (NSW)
compassionate grounds for disclosure .....36
compensation claims, see insurance and compensation
complaint handling .....36, **39**, 45
completeness of records.....26, 56
compliance tips .....17
computer screen displays, securing.....25
computerised records, see electronic records
conclusion of care, terminates rights of access .....46
confidentiality duties .....10, 59
consent to use personal information .....12-14, 29-33
contact tracing for infectious diseases .....54
contracted agencies.....17, 65
control of records .....56
conversations, discretion in.....25
copying records .....25
Coroner, authority to access records .....38
corrections to records, see records
crime, *see also* law enforcement agencies
obligations to disclose.....37-38
*Crimes Act*.....38


## D


data collections, access to .....58
data sponsors and custodians.....57
de-identified information.....12, 32
deceased patient records.....54-55
covered for 30 years.....12
FOI access to .....9
organ and tissue donors.....53-54
rights of access to end with death.....46
definitions .....**1-2**
delivery of information .....24-25
demonstrations, see training
Department of Community Services (NSW)
adoption information requests .....52

authority to access information .....37
information sharing with .....48
Department of Family and Community Services (Cth) 39
Department of Health (NSW).....40, 58
Department of Immigration and Multicultural and Indigenous Affairs (Cth).....40
Department of Veterans' Affairs (Cth).....39
direct mail, removal of details from.....51
directly related purposes.....28-29
Director-General
may release research data .....8
HIV-related information disclosed to.....32
public health and safety inquiries .....54
discharge referrals/summaries.....46
disciplinary policies for misconduct .....34
disclosure of personal health information .....27-40, *see also* records
disposal of records .....23, 56-57
DoCS, ***see*** Department of Community Services (NSW)
DOHEC .....58
drug and alcohol services .....53
duties of confidentiality .....10


## E


eDRS, see electronic records
EHR, see electronic records
electronic records .....59-60
discharge referrals/summaries .....24-25
information systems management.....17
linkage of .....44
privacy undertaking.....64
security of .....23-25
email, information transmitted by.....25
employers, requests for information by.....52
eMR, see electronic records
enquiries about patients .....50
Environmental Health Officers, powers of .....37
epidemiological data, release by Chief Health Officer ....8
Ethics Committee .....58
European Union Directive on Information .....43-44
*Evidence Act 1995:*.....59
expectations, reasonable .....28-29
express consent .....13
to eHR linkage .....44
to waive right to information .....19


## F


facsimile machine, information transmitted by.....24, 66
Family and Community Services Department (Cth).....39
family members
consultations with .....55
information access by.....47, 52
Federal Police, see law enforcement agencies
fees and charges for information access .....30, 42
fiduciary duties .....10
FOI requests .....9, 41
follow-up, makes anonymity impracticable .....22
*Freedom of Information Act 1989:*
requests under funding administrators .....9, 41
responsibilities under privacy law.....17
use of health information by .....32, 51


## G


General Disposal Authority .....17, 23
generally available publications.....33
genetic information .....11, 52
Government Insurance Office .....49
GPs, referrals to .....46
grants administrators, see funding administrators
group houses/hostels .....55
group sessions, records of .....55
guardians, *see* parents and guardians


## H


Health Administration Act 1982: .....8
Health Care Complaints Commission, powers of .....39
Health Department (NSW) .....40, 58
Health eLink, see electronic records
health facility closures.....57
Health Information Resources Directory .....57
health, preventing threats to .....31
Health Privacy Principles .....3, 6-7
HPP1: purposes of collection .....6, 18
HPP2: how to collect.....6, 18-19
HPP3: who to collect from .....6, 18-19
HPP4: individual to be made aware of collection .....6,19-21
HPP5: retention and security .....6, 23-25
HPP6: information held by organisations .....6
HPP7: access to information .....7
HPP8: amendment of information .....7
HPP9: accuracy.....7, 26
HPP10 & HPP11: use and disclosure.....7, 27-40, 58
HPP12: identifiers.....7, 43
HPP13: anonymity of information.....7
HPP14: transmittal outside NSW .....7, 43-44
HPP15: linkage of records .....7, 44
Health Professional Registration Boards .....4

health professionals, *see also* staff
registered, professional duties .....10
release of information about .....50
health records, *see* records
Health Records and Information Privacy Act 2002: ..3-4, 41
health service providers .....46-47
health service, seeks to use or disclose information ...30-31
Health Services Act.....18, 40
HIRD.....57
HIV-related information .....8-9, 32,
*see also* sexual health services
holders of information, defined .....12
HPPs, see Health Privacy Principles
HRECs .....58
HRIP Act, *see Health Records and Information Privacy Act 2002:*
Human Research Ethics Committees.....58

## I

identifiers assigned to individuals.....43
identity, deduced from information .....11-12
images of patients/clients .....50
Immigration and Multicultural and Indigenous Affairs, Department of (Cth).....40
implied consent .....13
incapacity
to give consent .....13
to understand .....19
Indigenous Australians .....51-52
infectious diseases, obligations regarding .....54
information, see personal health information; records
information systems managers .....7,
*see also* electronic records
informed consent .....12
insurance and compensation
documents required for claims .....30
information required for.....49-50
requests for genetic information .....52
Workcover claims .....39
Interagency Guidelines on Child Protection.....48
international transfers of information .....43-44
interpreters, use of .....49
interstate transfer of information.....43
interviews with police .....7
investigations of misconduct .....34-35
investigative agencies .....36

## J

Justice Health, prison officers in.....7

## K

key concepts .....**11-15**

## L

law enforcement agencies.....34-36, 47,
*see also* crime
legal claims, information required for .....49-50
legal representatives of patients/clients.....14-15, 49
legislation, see common law; names of Acts; privacy laws
linkage of records.....7, 44

## M

mail, information transmitted by .....24, 51
mailing lists, removal of details from.....51
management, use of health information in
.....16-17, 32-33, 58
Master Public Liability Insurance Policy.....49
media enquiries about patients.....50
medical examinations, disclosure to DoCS .....37, 48
medical practitioners, *see* GPs, referrals to; health professionals; staff
Mental Health Act 1990: .....8
Migration Act 1958 (Cth) .....40
Minister for Health, information required by.....40
minors, *see* children
misconduct, use of records to investigate .....34-35
missing persons, location of .....34
movement of records.....56

## N

next of kin, as authorised representative.....15
non-government organisations
bound by this manual .....4
commercial use of health information .....51
contracted agencies .....17, 65
use of public sector identifiers.....43
notifiable diseases, obligation to report .....54
NSW data collections.....57-58
NSW Department of Health Ethics Committee.....58
NSW Department of Health officers, powers of .....37
NSW Health data.....57
NSW Health Privacy intranet site.....17
NSW Healthnet, security of.....25
NSW Policy directives.....61
NSW Privacy Commissioner Statutory Guidelines 32-33, 58
NSW, transferring information out of .....43-44

## O

*Occupational Health and Safety Act 2000:* .....39
official visitors, powers of .....39
Ombudsman, powers of .....39
ongoing care, use of information in.....28
organ donors, information about .....53-54
other obligations .....**8-10**

## P

PANOC records.....48
paper records, security of .....23
parents and guardians
as authorised representatives .....14-15
parenting orders.....41
requests for information by .....48
patients/clients, see also deceased patient records
access to information.....**41-42**, 60
admission and registration forms for .....46
anonymity rights .....22
electronic records of.....59-60
enquiries about .....50
insurers of.....49-50
legal representatives.....14-15, 49
obligations to inform .....19-21
privacy of charts.....66
pro forma Privacy leaflet .....67-68
reasonable expectations of.....28-29
rights to privacy.....5
perinatal deaths, obligation to report .....40
personal affairs, information affecting .....41
personal health information .....11-12, *see also* records
'persons responsible' .....14-15, 49
photocopying .....25
Physical Abuse and Neglect of Children records.....48
police .....34-36, 47, *see also* crime
PPIP Act.....3, 45
practicability, defined.....15
practitioners, *see* health professionals
Premier, information required by.....40
primary purpose, use and disclosure for.....27
printing of records.....25
prison officers, access to prisoners' records 37
*Privacy and Personal Information Protection Act 1998:* 3, 45
Privacy Contact Officers.....16, 29
Privacy Intranet site.....17
privacy issues **46-58**
privacy laws 8-10, 62, *see also Health Records and Information Privacy Act 2002; Privacy and Personal Information Protection Act 1998:*
responsibilities under.....**16-17**
use and disclosure authorised by .....37
Privacy leaflets 17, 21,.....67-68
privacy notices attached to records.....55
Privacy pro formas.....63-65
privacy undertakings for electronic records .....59
*Private Hospitals and Day Procedure Centres Act* .....40
private organisations, see non-government organisations
pro forma leaflets.....17, 21, 67-68
professional obligations .....10
proofs of identity.....30, 42
protection of records.....6, **23-25**, 65
Public Health Act 1991:.....8-9
on HIV disclosure.....32
statutory reporting requirements .....40
public health and safety
disclosure in the interests of.....31-32, 35
inquiries into .....54
managing risks to.....54
public interest disclosures .....10
publications .....33

## Q

quality assessors, disclosure to.....28, 59
quality of health records.....55-56, 60

## R

reasonable expectations about information use.....28-29
reasonableness, defined.....15
records
access by family members .....47
access by third parties .....30
access to data collections .....58
amendment by patients/clients.....7, 42
collecting .....18-21
*Health Records and Information Privacy Act 2002:* .
.....3-4, 41
in group houses/hostels.....55
linkage of.....58
maintenance of .....23-25, 55-57
personal information in.....11-12
privacy issues .....46-58
pro forma privacy notice for.....66
storage and maintenance of .....23-25
use and disclosure.....27-40
registered health professionals.....10
registration forms .....46
*Registration of Births, Deaths and Marriages (Amendment) Act*.....40

removal of records.....56
repatriation clients, reporting deaths of.....39
reporting misconduct .....34-35
research, use of health information in.....8, 32-33, 58
responsibilities under privacy law.....16-17
retention of records.....23-25

## S

school children, see children
scope of this manual .....**4-7**
search warrants .....38, 47
secondary purpose, use and disclosure for.....27-32
security of information .....6, **23-25**, 65
serious criminal offences .....37-38, *see also* law enforcement agencies
service based policies and practices .....52-53
service providers.....5, 16-17
sexual assault victims
interviews with police.....47
policies for information management.....52-53
transfer of records.....56
sexual health services53, *see also* HIV-related information
*Social Security (Administration) Act 1999* (Cth).....39
staff, see also health professionals
anonymity rights of .....48
at risk of violence .....31
bound by this manual .....4
data rights of .....5
interviews with police.....47
privacy undertakings for electronic records.....59
release of information about .....50
responsibilities under privacy law .....16-17
role in data maintenance.....57
sanctions against disclosure by .....45
State Police, see law enforcement agencies
State Records Act 1998: .....9, 23
Statutory Guidelines, NSW Privacy Commissioner .....32-33, 58
statutory reporting requirements .....40
storage of records .....23-24, 56-57
students .....33, *see also* training
subcontractors.....7, 65
subpoenas.....38-39
supervisors ...16-17, *see also* management, use of health information in

## T

tapes of patients/clients .....50
Telehealth records.....55
telephone transmittal of information .....24
third parties
health service providers .....46-47
information collected from .....20
seeking access to information .....30
threats to health or welfare.....19-20, 31
timely consent .....13
tissue donors, information about.....53-54
Torres Strait Islander health information .....51-52
tracer notes .....56
training
in electronic records .....59
responsibilities under privacy law.....16
use of records during .....25, 32-33
transborder flows .....43-44
transfer of records .....56
transmittal of information .....24-25

## U

unlawful activity.....34-35, 37-38
unsolicited information, not covered by privacy law.....12
use of records .....**27-40**,*see also* records

## V

verbal communications, should be avoided.....20
Veterans' Affairs, Department of (Cth).....39
videotapes of patients/clients.....50
violent behaviour.....31, 35
voice mail, not to be used for information.....24

## W

ward details provided to enquirers.....50
welfare, threats to.....19-20, 31
Workcover, see insurance and compensation

# Notes

# Notes

**SHPN** (LLSB) 050066