



**NSW DEPARTMENT OF CORRECTIVE SERVICES**

**PRIVACY MANAGEMENT PLAN**

**February 2008**

**Prepared by the FOI & Privacy Unit**

**Document Classification: Public**

**TRIM Revision 20**

# Table of Contents

<b>ABBREVIATIONS AND ACRONYMS.....</b>	<b>4</b>
<b>1. INTRODUCTION .....</b>	<b>5</b>
Monitoring the Privacy Management Plan .....	5
Availability of the Privacy Management Plan .....	5
Contacting the Department of Corrective Services .....	5
Staff seeking advice .....	5
Further information.....	5
<b>2. DEFINITION OF PERSONAL AND HEALTH INFORMATION .....</b>	<b>7</b>
Personal information.....	7
Health information.....	8
<b>3. ACTIVITIES UNDERTAKEN BY THE DEPARTMENT .....</b>	<b>11</b>
Departmental structure.....	11
<b>4. TYPES OF FILES AND INFORMATION HELD BY THE DEPARTMENT .....</b>	<b>12</b>
Information systems and databases.....	13
Access by the Department to other agencies' information systems and databases .....	14
Registers .....	14
Disposal schedules.....	15
Record keeping .....	15
Types of personal information and health information collected, held, used and disclosed by the Department.....	16
Information in relation to offenders.....	16
Information in relation to staff, consultants and contractors.....	17
Information in relation to other persons.....	17
<b>5. THE INFORMATION PROTECTION PRINCIPLES (IPPS).....</b>	<b>18</b>
Exemptions from the Information Protection Principles.....	20
Exemptions written in the PPIP Act .....	20
Exemptions relating to law enforcement and related matters.....	20
Exemptions where non-compliance is lawfully authorised or required .....	21
Other exemptions where non-compliance would benefit the individual concerned.....	21
Other exemptions .....	21
Exemptions provided by Privacy Codes of Practice .....	22
Exemptions provided by section 41 directions .....	22
Exemptions provided by a regulation made under the PPIP Act .....	23
Corrupt disclosure and use of personal information by public sector officials .....	23
Access to and amendment of personal information .....	24
<b>6. THE HEALTH PRIVACY PRINCIPLES (HPPS).....</b>	<b>25</b>
Exemptions to the Health Privacy Principles.....	27
Exemptions written in the HRIP Act .....	27
Statutory guidelines issued under the HRIP Act.....	30
Health Records and Information Privacy Codes of Practice.....	31
Exemptions provided by section 62 directions .....	31
Exemptions written in a regulation made under the HRIP Act.....	31
Corrupt disclosure and use of health information by public sector officials and other offences .....	32
Access to and amendment of health information.....	32
<b>7. DISCLOSURE OF DEPARTMENTAL INFORMATION TO OTHER GOVERNMENT AGENCIES .....</b>	<b>34</b>

<b>8. DISCLOSURE OF INFORMATION WITH GOVERNMENT AGENCIES AND NON-GOVERNMENT ORGANISATIONS .....</b>	<b>35</b>
<b>9. THE <i>CRIMES (ADMINISTRATION OF SENTENCES) ACT 1999</i> AND OTHER LEGISLATION AFFECTING INFORMATION HELD BY THE DEPARTMENT OF CORRECTIVE SERVICES .....</b>	<b>36</b>
Crimes (Administration of Sentences) Act 1999 .....	36
Relevant provisions of the Crime (Administration of Sentences) Regulation 2001 .....	39
Other legislation.....	42
General Law.....	46
<b>10. SERVICE-WIDE POLICIES OR DOCUMENTS AFFECTING PERSONAL OR HEALTH INFORMATION HELD BY THE DEPARTMENT OF CORRECTIVE SERVICES..</b>	<b>47</b>
<b>11. DEPARTMENTAL POLICIES OR DOCUMENTS AFFECTING PERSONAL OR HEALTH INFORMATION HELD BY THE DEPARTMENT OF CORRECTIVE SERVICES..</b>	<b>48</b>
<b>12. DISSEMINATION OF POLICIES AND PROCEDURES TO STAFF OF THE DEPARTMENT OF CORRECTIVE SERVICES.....</b>	<b>49</b>
<b>13. CONSULTANTS AND CONTRACTORS .....</b>	<b>50</b>
<b>14. THE INTERNAL REVIEW PROCESS .....</b>	<b>51</b>

## Abbreviations and Acronyms

ACO – Assistant Commissioner Order

AD – Access Directions

ADT – Administrative Decisions Tribunal

BIMS – Business Integrated Management System

BOCSAR – Bureau of Crime Statistics and Research

Cats.i – Customer Assistance Tracking System

Code – Part 5 of the *Privacy Code of Practice (General) 2003*

CIMS – Corporate Information Management System

COPS – Computerised Operational Policing System

Ellipse – brand name not acronym

FOI – Freedom of Information

FOI Act – *Freedom of Information Act 1989*

Groupwise – brand name not acronym

Health Code – *Health Records and Information Privacy Code of Practice 2005*

HPP – Health Privacy Principle

HRIP Act – *Health Records and Information Privacy Act 2002*

IC&T – Information Communication & Technology

Information – used in this Plan to refer to personal and/or health information

IPP – Information Protection Principle

ISYS – brand name not acronym

MIMS – MINCOM Information Management System (MINCOM is a brand name not acronym)

MOU – memorandum of understanding

NCIS – National Coronial Information System

NSW – New South Wales

OIMS – Offender Integrated Management System

OPM – Operations Procedures Manual

Plan – The Department of Corrective Services' Privacy Management Plan

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

Privacy Legislation – refers to both the PPIP Act and the HRIP Act

Records Act – *State Records Act 1998*

SORC – Serious Offenders Review Council

SPA – NSW State Parole Authority

The Department – The Department of Corrective Services

TRIM – Tower Record Information Management

## 1. Introduction

- 1.1 This Privacy Management Plan (Plan) is intended to satisfy the requirements of section 33(2) of the *Privacy and Personal Information Protection Act 1998* (PIIP Act), which requires:
- a) the devising of policies and practices to ensure compliance by the agency with the requirements of this Act or the *Health Records and Information Privacy Act 2002* (HRIP Act), if applicable,
  - b) the dissemination of those policies and practices to persons within the agency,
  - c) the procedures that the agency proposes to provide in relation to internal review under Part 5,
  - d) such other matters as are considered relevant by the agency in relation to privacy and the protection of personal information held by the agency.
- 1.2 The Department of Corrective Services (Department) is committed to respecting the privacy rights of individuals.

### Monitoring the Privacy Management Plan

- 1.3 The Department's Freedom of Information (FOI) & Privacy Unit monitors the Plan on an ongoing basis. Changes to the Plan are made when necessary. The Plan is reported on in the Department's Annual Report.

### Availability of the Privacy Management Plan

- 1.4 The Plan is available for public inspection or purchase (free of charge) as a policy document in accordance with section 15 of the *Freedom of Information Act 1989* (FOI Act). The Plan is available on the Department's Internet and intranet sites. The Internet address is: [www.dcs.nsw.gov.au](http://www.dcs.nsw.gov.au).

### Contacting the Department of Corrective Services

- 1.5 All privacy matters, including access to and amendment of documents/information, should be referred to the Manager of the Department's FOI & Privacy Unit. The Manager can be contacted on telephone: (02) 8346 1067. The Department's Internet address is: [www.dcs.nsw.gov.au](http://www.dcs.nsw.gov.au).

### Staff seeking advice

- 1.6 All staff seeking advice regarding privacy matters, including the interpretation of legislation must contact the FOI & Privacy Unit. The Manager can be contacted on telephone: (02) 8346 1067 and the FOI & Privacy Project Officer on telephone: (02) 8346 1476.

### Further information

- 1.7 Further information on the PIIP Act and the HRIP Act can be found at the website of

Privacy NSW:

[http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll\\_pnsw.nsf/pages/PNSW\\_index](http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_index)

## 2. Definition of Personal and Health Information

### Personal information

2.1 “Personal information” is defined by section 4(1) of the PPIP Act as, “information or an opinion (including information or an opinion forming part of a database and whether or not recorded in material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion”. Section 4(2) provides that personal information “includes such things as an individual’s fingerprints, retina prints, body samples or genetic characteristics”.

2.2 Section 4(3) of the PPIP Act provides “personal information” does not include:

- information about a person who has been deceased for more than 30 years;
- information contained in a publicly available document;
- information about a witness who is included in a witness protection program under the *Witness Protection Act 1995* or is subject to witness protection arrangements made under an Act;
- information arising from a warrant issued under the *Telecommunications (Interception) Act 1979* (Cth);
- information obtained in a protected disclosure within the meaning of the *Protected Disclosures Act 1994* or collected during the course of an investigation arising out of a protected disclosure;
- information arising out of, or in connection with, an authorised operation within the meaning of the *Law Enforcement (Controlled Operations) Act 1997*;
- information arising out of a Royal Commission or Special Commission of Inquiry;
- information arising out of a complaint made under Part 8A of the *Police Service Act 1990*;
- information that is contained in a document of a kind referred to in clause 1 or 2 of Schedule 1 (restricted documents) to the *Freedom of Information Act 1989*;
- information or opinion about suitability for appointment or employment as a public sector official;
- information about an individual that is obtained about an individual under Chapter 8 of the *Adoption Act 2000*; or
- information that is of a class, or is contained in a document of a class, prescribed by the regulations.

Section 4A of the PPIP Act states that the definition of personal information in section 4 does not include health information within the meaning of the HRIP Act.

Clause 4 of the *Privacy and Personal Information Protection Regulation 2005* states that for the purposes of section 4 of the PPIP Act, the following information is not personal information:

- information about an individual that is contained in a document kept in a library, art gallery or museum for the purposes of reference, study or exhibition,
- information about an individual that is contained in a State record under the control of the State Records Authority [now known as State Records NSW or State Records Authority of NSW] that is available for public inspection in accordance with the *State Records Act 1998*,
- information about an individual that is contained in archives within the meaning of the *Copyright Act 1968* of the Commonwealth.

2.3 Privacy NSW has advised that:

“A person’s identity can be reasonably ascertained if it is possible to pin-point the individual concerned from another readily available source, for example a public register or phone book.

The definition does not generally cover information about a number of people, which has been aggregated or presented in a statistical form. It would not usually cover information or opinions about corporations or organisations, or information about individuals when they are acting in a public or business capacity although the borderline may not always be clear. For example some information about the business activities of sole traders, family businesses or farmers could still be regarded as personal.”

## Health information

2.4 “Health information” is a specific type of personal information. The collection, storage, use and disclosure of health information is regulated by the HRIP Act. Section 6 of the HRIP Act defines health information as:

- (a) personal information that is information or an opinion about:
  - (i) the physical or mental health or a disability (at any time) of an individual, or
  - (ii) an individual’s express wishes about the future provision of health services to him or her, or
  - (iii) a health service provided, or to be provided, to an individual, or
- (b) other personal information collected to provide, or in providing, a health service, or
- (c) other personal information about an individual collected in connection with the donation, or intended donation, of an individual’s body parts, organs or body substances, or

- (d) other personal information that is genetic information about an individual arising from a health service provided to the individual in a form that is or could be predictive of the health (at any time) of the individual or of any sibling, relative or descendant of the individual,

but does not include health information, or a class of health information or health information contained in a class of documents, that is prescribed as exempt health information for the purposes of the HRIP Act generally or for the purposes of specified provisions of the HRIP Act.

2.5 Subsections 5(1) and (2) of the HRIP Act, adopt the same definition of personal information as subsections 4(1) and (2) of the PPIP Act. Section 5(3) of the HRIP Act specifies the following information as not included within the meaning of “personal information”:

- Information about an individual who has been dead for more than 30 years.
- Information about an individual that is contained in a generally available publication.
- Information about an individual that is contained in a document kept in a library, art gallery or museum for the purposes of reference, study or exhibition.
- Information about an individual that is contained in a State record under the control of the State Records Authority [now known as State Records NSW or State Records Authority of NSW] that is available for public inspection in accordance with the *State Records Act 1998*.
- Information about an individual that is contained in archives within the meaning of the *Copyright Act 1968* of the Commonwealth.
- Information about a witness who is included in a witness protection program under the *Witness Protection Act 1995* or who is subject to other witness protection arrangements made under an Act.
- Information about an individual arising out of a warrant issued under the *Telecommunications (Interception) Act 1979* of the Commonwealth.
- Information about an individual that is contained in a protected disclosure within the meaning of the *Protected Disclosures Act 1994*, or that has been collected in the course of an investigation arising out of a protected disclosure.
- Information about an individual arising out of, or in connection with, an authorized operation within the meaning of the *Law Enforcement (Controlled Operations) Act 1997*.
- Information about an individual arising out of a Royal Commission or Special Commission of Inquiry.
- Information about an individual arising out of a complaint made under Part 8A of the *Police Service Act 1990*.
- Information about an individual that is contained in a document of a kind referred to

in clause 1 or 2 of Schedule 1 (Exempt documents) to the *Freedom of Information Act 1989* (i.e. Cabinet documents or Executive Council documents).

- Information or an opinion about an individual's suitability for appointment or employment as a public sector official.
- Information about an individual that forms part of an employee record (within the meaning of the *Privacy Act 1988* of the Commonwealth) about the individual held by a private sector person.
- Information about an individual that is of a class, or is contained in a document of a class, prescribed by the regulations.

As of the date of this Plan, the *Health Records and Information Privacy Regulation 2006* does not prescribe any class of documents as being exempt.

### 3. Activities undertaken by the Department

3.1 Personal and health information may be used in any of the Department's activities. Some activities are listed below:

- the maintenance of safe and secure correctional facilities;
- the care and control of offenders held in correctional facilities and other establishments such as cell areas of court complexes;
- the administration of sentences imposed upon offenders by sentencing authorities;
- supervision of offenders in the community;
- assessment and case management of offenders in correctional facilities and in the community;
- Corrective Service Industries;
- Work release programs;
- the provision of specialist programs to assist offenders such as the Drug Court program, violence prevention strategies, NSW Housing and Human Services Accord, Sex Offenders' program, drug and alcohol program, education and vocational training;
- the preparation of a variety of reports in respect of proceedings before sentencing authorities and statutory bodies such as the NSW State Parole Authority (SPA) and the Serious Offenders Review Council (SORC);
- research, evaluation and statistical activities of the department;
- investigative and complaint-handling activities; and
- restorative justice programs including victim-offender conferencing and protective mediation.

#### Departmental structure

3.2 For information on the structure of the Department of Corrective Services, please refer to the Department's latest Annual Report which is available on the Department's Internet site: [www.dcs.nsw.gov.au](http://www.dcs.nsw.gov.au).

SPA, SORC and the Junee Correctional Centre are not considered part of the Department for the purposes of privacy legislation. Junee Correctional Centre is managed by a private sector organisation and is currently covered by the Commonwealth *Privacy Act 1988* and the private sector provisions of the HRIP Act. All enquiries regarding privacy matters at Junee should be made directly with that Centre on telephone: (02) 6930 5522.

## 4. Types of files and information held by the Department

4.1 The Department has 25 file classifications as follows:

- Asset management
- Case management
- Community-based management
- Compensation
- Corporate communications
- Correctional education
- Correctional industries
- Custody management
- Establishment
- Financial management
- Fleet management
- Government relations
- Industrial relations
- Information management
- Intelligence
- Legal services
- Occupational health and safety (OH&S)
- Personnel
- Procurement
- Property management
- Research
- Staff development
- Strategic management
- Technology and communications
- Victim services

Following are some examples of the specific types of files within the file classifications:

<b>File Type</b>	<b>General Contents of File</b>
Assessment	Information about an offender prepared by the Probation and Parole Service.
Case Management	Information about an inmate prepared by the inmate's case management team and other documents about the inmate's day-to-day imprisonment.
Case History	Information in relation to Community Offender Services including the NSW Housing and Human Services Accord.

Community Service Order	Information about an offender prepared by the Probation and Parole Service.
Employer	Information about employers participating in the Work Release Program.
Fine Default	Information about an offender prepared by the Probation and Parole Service.
High Security Inmate Management	Information about an inmate managed by the High Security Inmate Management Committee.
Leave	Information about an inmate's participation in day or weekend leave.
Offender	Information about an inmate usually in relation to correspondence between the inmate and the Department.
Part-time Teacher	Information about a part-time teacher working for the Department.
Periodic Detention	Information about offenders in the Periodic Detention Program.
Personal ("P" file)	Information about an employee prepared by Departmental staff in regard to personnel matters.
Psychology	Information about an inmate prepared by a Departmental psychologist.
Serious Offenders Review Council	Information about a serious offender, or other inmate who comes within the jurisdiction of the SORC.
State Parole Authority	Information about an inmate eligible for parole.
Supervision/Case History	Information about an offender prepared by the Probation and Parole Service.
Warrant	Information about an inmate – eg. Warrants, court appearances.
Work Release	Information about an inmate's participation in the Work Release Program or Education Leave.

4.2 The Department does not hold "medical" files for inmates, as JH is responsible for providing medical services to inmates. JH is a statutory health corporation established under the *Health Services Act 1997* and is funded by NSW Health. JH keeps its own files and its records management unit may be contacted on telephone (02) 9289 5011. However, the Department employs psychologists who maintain psychology files on inmates, which contain their personal and health information. Other Departmental files may contain health information.

### Information systems and databases

4.3 The Department maintains various databases and software applications, which contain personal and health information. The main databases are: the Offender Integrated Management System (OIMS), Tower Record Information Management (TRIM), MINCOM Information Management System (MIMS), ISYS, GroupWise, Ellipse and the Customer Assistance Tracking Scheme (Cats.i).

- 4.4 OIMS contains information about offenders such as names, dates of birth, sentence and case management information. A warning about unauthorised access, use and disclosure of information contained in OIMS is displayed to officers whenever they log into the database.
- 4.5 TRIM is the Department's primary records and electronic document management software. It is used to register, store and manage any document or record, physical or electronic, created or used by the Department's staff in the course of conducting the Department's business.
- 4.6 MIMS is a corporate information management application for financial records.
- 4.7 ISYS (brand name not acronym) contains intelligence holdings on offenders.
- 4.8 GroupWise is a corporate e-mail and calendar application used for preparing, sending, receiving and storing electronic communications.
- 4.9 Ellipse is a corporate standard human resources and financial system, which is used for assets and works, supply and logistics, financial and human resources management.
- 4.10 Cats.i is the complaints management system used to record, manage and report on complaints against officers of the Department, non-Departmental employees such as JH personnel, teachers, contractors, religious workers and local management issues.
- 4.11 There are also many other local electronic information systems used on computers throughout the Department that may contain personal and health information.

### **Access by the Department to other agencies' information systems and databases**

- 4.12 The NSW Attorney General's Department's Court System.  
(Permitted by section 41 direction on information transfers between public sector agencies)
- 4.13 The Police Service's Computerised Operational Policing System (COPS). Use of that database is governed by the "NSW Police Service External Client 'On-Line' Access Policy". (Permitted by section 27 of the PPIP Act)

### **Registers**

- 4.14 The Department does not hold any public registers within the meaning of section 3 of the PPIP Act. A public register is defined in the PPIP Act as "a register of personal information that is required by law to be, or is made, publicly available or open to public inspection (whether or not on payment of a fee)".
- 4.15 The Department does, however, maintain the Victims' Register. Section 256 of the *Crimes (Administration of Sentences) Act 1999* provides for the Victims' Register. Section 256(2) of the same Act provides that the Victims' Register is to record the "names of victims of offenders who have requested that they be given notice of the possible parole of the offender concerned".
- 4.16 Pursuant to section 14 of the *Crimes (Interstate Transfer of Community Based Services) Act 2004* the Department is required to maintain a register of interstate sentences. Schedule 1 of the *Crimes (Interstate Transfer of Community Based Services) Regulation 2004* sets out the type of personal information about offenders required to be entered in the register.

4.17 The Department is also required to maintain a register of access directions in accordance with section 61 of the *State Records Act 1998*. This register must be available to any person free of charge and can be found on the State Records NSW website:

[http://www.records.nsw.gov.au/archives/corrective\\_services\\_department\\_of\\_2993.asp](http://www.records.nsw.gov.au/archives/corrective_services_department_of_2993.asp)

Currently three access directions (AD) have been made, but only one, as follows, relates directly to personal and health information:

AD No.	Scope	Duration	Direction
303	Records relating to individual offenders and staff	70 years	Closed *

\* Records that fall within AD 303 are closed for general public access; however, FOI applications may still be made for access to documents relating to individuals and staff, even if those documents are less than 70 years old.

Under the *State Records Act 1998* (Records Act), the Department may make, change or revoke AD at any time. Some of the Department's records, which are at least 30 years old, are held by State Records NSW while the Department itself holds some records. For more information regarding AD, refer to the Department's "Public Access to Records, Documents, Personal and Health information" document, which is available on the Department's intranet and Internet sites.

## Disposal schedules

4.18 The Records Act clearly defines the disposal schedules by which the Department may legally destroy files, which are of no further use. All records created in the Department are subject to the provisions of the Records Act. It is an offence to dispose of records other than in accordance with the Records Act.

## Record keeping

4.19 The Records Act requires public officials to "make and keep full and accurate records" of their business activities.

The NSW Public Sector Code of Conduct requests that public officials should "maintain adequate documentation to support any decisions made" in the performance of their duties.

The Ombudsman's Good Conduct and Administrative Practice Guidelines for Public Authorities and Officials states that "public officials must make and create records to support accountability and corporate memory".

All staff are responsible for correctly maintaining records as they represent the Department's corporate memory. The "Corporate Records and Archival Management Policy and Procedures Manual" establishes a framework for the management of the Department's documents and records.

Section 21 of the Department's Operations Procedures Manual (OPM) instructs staff on records management. It advises that it is important that government agencies keep efficient records management systems so that their staff may quickly find and retrieve documents.

All departmental staff must act responsibly, objectively and professionally in the statements and comments they attach to files.

The OPM also advises comments and statements on offenders' files must be relevant to the management of the offender. The comments and statements must make clear distinctions between facts – that is, what you have seen with your own eyes or what you have heard with your own ears and opinions or assumptions.

ACO 97/101, available on the Department's intranet, reminds staff that comments and statements on files must be confined to statements of fact or opinion. This is particularly important where staff are required to evaluate people in some way, for instance, in relation to their work performance, or the eligibility for some benefit such as emergency housing, or in the management of offenders. Access to all documents held by the Department may be granted to applicants under the FOI Act. Access to documents that are covered by the FOI Act may only be denied if there is an applicable exemption or section available under the FOI Act. Possible embarrassment to the Department is not grounds for denying access to a document.

## **Types of personal information and health information collected, held, used and disclosed by the Department**

4.20 The following lists are indicative of the types of personal and health information collected, held, used and disclosed by the Department:

### **Information in relation to offenders**

- name, alias, date of birth
- criminal antecedents
- transcripts from court proceedings
- police documents
- fingerprints
- information regarding any identifying features of inmates (such as tattoos)
- physical descriptions
- photographs
- biometric information
- video and close circuit television footage
- details regarding an offender's next-of-kin
- details of an offender's address and domestic circumstances
- family history
- details of medical conditions; disabilities; psychological and psychiatric history; self-harm attempts
- psychological test results
- copies of psychiatric, psychological and other medical reports
- details of substance abuse history
- drug test results
- information about associates and co-offenders
- ethnic or racial background
- languages spoken
- religious beliefs
- employment history details
- income and finances

- intelligence information

### **Information in relation to staff, consultants and contractors**

- name, address, date of birth, telephone number, qualifications and educational history, employment history, salary details, bank account details, tax file number, ethnic or racial background, disabilities and languages spoken
- photographs
- medical assessment reports and medical certificates
- workers compensation details
- reports concerning allegations of misconduct or corruption
- details of any criminal proceedings
- drug test results
- debt recovery documents such as garnishee orders, child support agency orders
- video and close circuit television footage
- mobile phone records
- intelligence information

### **Information in relation to other persons**

- personal details of visitors to correctional centres (name, address, date of birth, telephone number, relationship with inmate and identification details)
- biometric algorithms and photographic images of visitors
- criminal record checks of sponsors for inmates applying for day and weekend leave and for potential employers in the work release program
- intelligence information about visitors who may be a threat to the security and good order of correctional centres
- vehicle registration checks
- video and close circuit television footage
- information about victims of crime
- information provided to probation and parole officers
- information provided by offenders

## 5. The Information Protection Principles (IPPs)

5.1 The 12 IPPs, which are set out in sections 8 - 19 inclusive of the PPIP Act, are summarised as follows:

### Collection

**IPP 1** Lawful – the Department may only collect personal information for a lawful purpose that is directly related to its functions and activities and is reasonably necessary for that purpose.

**IPP 2** Direct – the Department must only collect personal information directly from the person concerned, unless it is unreasonable or impracticable to do so.

**IPP 3** Open – the Department must take such steps as are reasonable in the circumstances to ensure that, before the information is collected, or as soon as practicable after collection, the individual to whom the information relates is made aware that the information is being collected; the purpose for which it is being collected; the intended recipients; whether the supply of the information is required by law or is voluntary; the existence of any right of access to, and correction of the information; as well as the name and address of the agency that holds the information.

**IPP 4** Relevant – the Department must take such steps as are reasonable in the circumstances to ensure that any information collected is relevant to the purposes for which it is collected, is not excessive, is accurate, up to date and complete. The Department must take such steps as are reasonable in the circumstances to ensure that the collection does not unreasonably intrude into the personal affairs of the individual.

### Retention & Security

**IPP 5** Security – the Department must take such security safeguards as are reasonable in the circumstances to ensure that personal information is stored securely. Personal information should not be kept any longer than necessary and disposed of securely. The information should be protected from unauthorised access, use, modification or disclosure. When it is necessary to give the information to a person in connection with the provision of a service to the Department, all reasonable steps must be taken by the Department to prevent unauthorised use or disclosure of the information.

### Transparency

**IPP 6** Transparent – the Department must take such steps as are reasonable in the circumstances to enable a person to ascertain what personal information about them is held, why it is being used and any right they have to access it.

## Access & Amendment

- IPP 7** Accessible – the Department must allow people to access their personal information without unreasonable delay or expense.
- IPP 8** Correct – the Department must allow people to update, correct or amend their personal information where appropriate.

## Accuracy

- IPP 9** Accurate – the Department must take such steps as are reasonable in the circumstances to ensure that the personal information is relevant, accurate, up to date, complete and not misleading before using it.

## Use

- IPP 10** Limited use – the Department must not use personal information for a purpose other than the purpose for which it was collected unless the person consents to such use or the other purpose is a directly related purpose for which the person would reasonably expect the organisation to use the information. Otherwise, you generally need their consent.

## Disclosure

- IPP 11** Limited disclosure – only disclose personal information for the purpose for which it was collected, or a directly related purpose that the person would expect. Otherwise, you generally need their consent.
- IPP 12** Restrictions – the Department must not disclose personal information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities unless the disclosure is necessary to prevent a serious and imminent threat to the life or health of the individual concerned or another person.

The Department must not disclose personal information to any person or body who is in a jurisdiction outside New South Wales or to a Commonwealth agency unless a relevant privacy law applies, or the disclosure is permitted under a privacy code of practice.

## Exemptions from the Information Protection Principles

5.2 There are four sources of exemptions to the IPPs:

1. Exemptions written in the PPIP Act itself
2. Exemptions written in a privacy code of practice, made by the Attorney General under the PPIP Act
3. Exemptions written in a public interest direction, made by the Privacy Commissioner under section 41 of the PPIP Act
4. Exemptions written in a regulation made by the Attorney General under the PPIP Act.

### Exemptions written in the PPIP Act

Those exemptions pertinent to the Department are as follows:

#### Exemptions relating to law enforcement and related matters

5.3 The Department is defined as a law enforcement agency by section 3(f) of the PPIP Act. Section 23 deals with exemptions relating to law enforcement agencies as follows:

5.4 Section 23(1) provides that “a law enforcement agency is not required to comply with section 9 (IPP 2) if compliance by the agency would prejudice the agency’s law enforcement functions”

5.5 Section 23(2) provides that “a public sector agency (whether or not a law enforcement agency) is not required to comply with section 9 (IPP 2) if the information concerned is collected in connection with proceedings (whether or not actually commenced) before any court or tribunal”.

5.6 Section 23(3) provides that “a public sector agency (whether or not a law enforcement agency) is not required to comply with section 10 (IPP 3) if the information concerned is collected for law enforcement purposes. However, this subsection does not remove any protection provided by any other law in relation to the rights of accused persons or persons suspected of having committed an offence”.

5.7 Section 23(4) provides that “a public sector agency (whether or not a law enforcement agency) is not required to comply with section 17 (IPP 10) if the use of the information concerned for a purpose other than the purpose for which it was collected is reasonably necessary for law enforcement purposes or for the protection of the public revenue”.

5.8 Section 23(5) provides that “a public sector agency (whether or not a law enforcement agency) is not required to comply with section 18 (IPP 11) if the disclosure of the information concerned:

- (a) is made in connection with proceedings for an offence or for law enforcement purposes (including the exercising of functions under or in connection with the *Confiscation of Proceeds of Crime Act 1989* or the *Criminal Assets Recovery Act 1990*), or

- (b) is to a law enforcement agency (or such other person or organisation as may be prescribed by the regulations) for the purposes of ascertaining the whereabouts of an individual who has been reported to a police officer as a missing person, or
- (c) is authorised or required by subpoena or by search warrant or other statutory instrument, or
- (d) is reasonably necessary:
  - (i) for the protection of the public revenue, or
  - (ii) in order to investigate an offence where there are reasonable grounds to believe that an offence may have been committed”.

5.9 However, section 23(6) provides that “nothing in subsection (5) requires a public sector agency to disclose personal information to another person or body if the agency is entitled to refuse to disclose the information in the absence of a subpoena, warrant or other lawful requirement”.

5.10 Section 23(7) provides that “a public sector agency (whether or not a law enforcement agency) is not required to comply with section 19 (IPP 12) if the disclosure of the information concerned is reasonably necessary for the purposes of law enforcement in circumstances where there are reasonable grounds to believe that an offence may have been, or may be, committed”.

### **Exemptions where non-compliance is lawfully authorised or required**

5.11 Section 25 provides that “a public sector agency is not required to comply with sections 9, 10, 13, 14, 15, 17, 18 or 19 (IPPs 2, 3, 6, 7, 8, 10, 11 and 12) if:

- (a) the agency is lawfully authorised or required not to comply with the principle concerned, or
- (b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*)”.

### **Other exemptions where non-compliance would benefit the individual concerned**

5.12 Section 26(1) provides that “a public sector agency is not required to comply with sections 9 or 10 (IPPs 2 or 3) if compliance by the agency would, in the circumstances, prejudice the interests of the individual to whom the information relates”.

Section 26(2) further provides that “a public sector agency is not required to comply with sections 10, 18 or 19 (IPPs 2, 10 and 11) if the individual to whom the information relates has expressly consented to the agency not complying with the principle(s) concerned”.

### **Other exemptions**

5.13 Pursuant to section 28(3) of the PPIP Act, “nothing in sections 17, 18 or 19 (IPPs 10, 11 or 12) prevents or restricts the disclosure of information:

- a) by a public sector agency to another public sector agency under the administration of the same Minister if the disclosure is for the purposes of informing that Minister about any matter within that administration, or
- b) by a public sector agency to any public sector agency under the administration of the Premier if the disclosure is for the purpose of informing the Premier about any matter”.

## Exemptions provided by Privacy Codes of Practice

5.14 Privacy codes of practice which modify the application of the IPPs may be made under Part 3 of the PPIP Act. The Department has a Privacy Code of Practice (Code), which is incorporated into Part 5 of the *Privacy Code of Practice (General) 2003*. The Code provides for a number of exemptions to the IPPs. The Code is available on the NSW legislation website: <http://www.legislation.nsw.gov.au> or the Privacy NSW website at:

[http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll\\_pnsw.nsf/pages/PNSW\\_03\\_ppipcodes](http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_03_ppipcodes)

Further details about the exemptions in the Code are discussed in sections 7 and 8 of this Plan.

5.15 Currently the following other Privacy Codes of Practice are also applicable to the Department:

- Privacy Code of Practice: Bureau of Crime Statistics and Research
- Privacy Code of Practice: Office of the Director of Public Prosecutions
- Privacy Code of Practice for the NSW Public Sector Workforce Profile

The above three Codes of Practice may be viewed on Privacy NSW’s website at:

[http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll\\_pnsw.nsf/pages/PNSW\\_03\\_ppipcodes](http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_03_ppipcodes)

5.16 Part 4 of the *Privacy Code of Practice (General) 2003* deals with Human Services. Part 4 is not applicable to this Department. The Department of Premier and Cabinet has deemed this Department to be a justice agency and not a human services agency. The types of health services listed in section 4(1) of the health code are not this Department’s core business. Notwithstanding, for the purposes of the NSW Housing and Human Services Accord, references to human services explicitly include the Department’s Community Offender Services.

Further details about the Accord are discussed in section 8 of this Plan.

## Exemptions provided by section 41 directions

5.17 The Privacy Commissioner may issue directions under section 41 of the PPIP Act which exempt a public sector agency from compliance with an IPP or a privacy code of practice, or modify the application of a principle or a code to the public sector agency as specified in the direction. Section 41 directions may be viewed on the Privacy NSW website at:

[http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll\\_pnsw.nsf/pages/PNSW\\_index](http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_index)

As of the date of this Plan, the following section 41 directions are applicable to the Department:

- Direction relating to Anti-Social Behaviour Pilot Project
- Direction on Child Protection Watch Team
- Direction relating to the Redfern Waterloo Partnership Project
- Direction on Disclosures of Information by the New South Wales Public Sector to the National Coronial Information System (NCIS)
- Direction on Collection and Disclosure for Research Purposes
- Direction on Disclosure of Information to Victims of Crime
- Direction on Processing of Personal Information by Public Sector Agencies in Relation to their Investigative Functions
- Direction on Information Transfers Between Public Sector Agencies

## **Exemptions provided by a regulation made under the PPIP Act**

5.18 The *Privacy and Personal Information Protection Regulation 2005* makes exemptions in relation to privacy management plans as follows:

### **“5 Exemptions in relation to privacy management plans**

(1) A public sector agency is exempt from the provisions of section 33 of the Act if:

- (a) the staff of the relevant agency are part of the staff of another public sector agency, or
- (b) the Minister has, by order published in the Gazette, declared that the relevant agency is taken to be included in another public sector agency, and the privacy management plan of that other agency states that the plan extends to the relevant agency.”

5.19 The regulation also states that a public sector agency is exempt from sections 17-19 of the Act (IPPs 10 – 12) in respect of disclosure of personal information to an Aboriginal Trust Fund Repayment (ATFR) Scheme agency (Department of Aboriginal Affairs, the State Records Authority or the Premier’s Department) in connection with the implementation and operation of the ATFR Scheme established by the NSW Government.

## **Corrupt disclosure and use of personal information by public sector officials**

5.20 Section 62 of the PPIP Act prohibits disclosure of personal information by public sector officials, which is not done in accordance with the performance of their official duties. Intentional disclosure or use of personal information by public sector officials is an offence punishable by up to 100 penalty units or imprisonment for two years, or both.

5.21 Section 63 of the PPIP Act prohibits a person from inducing or attempting to induce a public sector official (by way of a bribe or other similar corrupt conduct) to disclose any personal information about another person to which the official has or had access in the exercise of his or her official functions. This is an offence punishable by up to 100 penalty units or imprisonment for two years, or both.

A reference to a public sector official includes a reference to a person who was formerly a public sector official.

## Access to and amendment of personal information

- 5.22 The Department has prepared a paper entitled, *Public Access to Records, Documents, Personal Information and Health information*. The paper, among other things, explains how personal information held by the Department, or held on behalf of the Department by State Records Authority of NSW, may be obtained. The paper is available on the Department's intranet and Internet sites.
- 5.23 Under section 16 of the FOI Act, you have the right to apply to the Department for access to any documents held by it about you. Under section 39 of the FOI Act you may apply to the Department to have any document held by it about you amended if you consider that the information contained in the document is incomplete, incorrect, out of date or misleading.
- 5.24 You also have access and amendment rights under the PPIP Act, nevertheless, section 20(5) of the PPIP Act provides:

“Without limiting the generality of section 5, the provisions of the FOI Act that impose considerations or limitations (however expressed) with respect to any matter referred to in section 13, 14 or 15 are not affected by this Act, and those provisions continue to apply in relation to any such matter as if those provisions were part of this Act.”

This sub-section has the effect of importing into any decision regarding sections 13 to 15 of PPIP Act (otherwise known as IPPs 6, 7 and 8), provisions of the FOI Act, which impose considerations or limitations with respect to any matter referred to in sections 13 to 15. Those matters referred to in sections 13 to 15 respectively are as follows:

- Permitting persons to determine whether the agency holds personal information
- Right of access to information held by the agency
- Right of alteration of personal information.

Accordingly, any request made under sections 13 to 15 of the PPIP Act will be largely processed as if it had been made under the FOI Act; however, the appeal rights differ.

- 5.25 For details on how to make an application under the FOI Act, contact the FOI & Privacy Unit or refer to the Department's Internet site: [www.dcs.nsw.gov.au](http://www.dcs.nsw.gov.au).

Section 5 of the PPIP Act states:

### **“5 Freedom of Information Act 1989 not affected**

- (1) Nothing in this Act affects the operation of the *Freedom of Information Act 1989*.
- (2) In particular, this Act does not operate:
  - (a) to modify any exemption under the *Freedom of Information Act 1989*, or
  - (b) to lessen any obligations under that Act in respect of a public sector agency.”

## 6. The Health Privacy Principles (HPPs)

6.1 The 15 HPPs, which are set out in Schedule 1 to the HRIP Act, are summarised as follows:

### Collection

- HPP 1** Lawful – an organisation may only collect health information for a lawful purpose that is directly related to its functions and activities and is reasonably necessary for that purpose.
- HPP 2** Relevant – an organisation must take such steps as are reasonable in the circumstances to ensure that any health information collected is relevant to the purposes for which it is collected, not excessive, is accurate, up to date and complete. An organisation must take such steps as are reasonable in the circumstances to ensure that the collection does not unreasonably intrude into the personal affairs of the individual.
- HPP 3** Direct – an organisation must only collect health information directly from the person concerned, unless it is unreasonable or impracticable to do so.
- HPP 4** Open – an organisation must take such steps as are reasonable in the circumstances to inform the person as to why the health information is being collected, what will happen to the health information, and who else might see it. An organisation must tell the person how they can see and correct their health information and the main consequences if they decide not to provide their information to the organisation. If an organisation collects health information about a person from someone else, it must take any steps that are reasonable in the circumstances to ensure that the person has been notified as above.

### Storage

- HPP 5** Secure – an organisation must take such security safeguards as are reasonable in the circumstances to ensure that health information is stored securely. Health information should not be kept any longer than necessary and disposed of securely. Information should be protected from unauthorised access, use, modification or disclosure. When it is necessary to give the information to a person in connection with the provision of a service to the organisation, all reasonable steps must be taken by the organisation to prevent unauthorised use or disclosure of the information.

## Access & Accuracy

- HPP 6** Transparent – an organisation must take such steps as are reasonable in the circumstances to enable a person to ascertain what health information about them is held, why it is being used and any right they have to access it.
- HPP 7** Accessible – an organisation must allow people to access their health information without unreasonable delay or expense.
- HPP 8** Correct – an organisation must allow people to update, correct or amend their health information where appropriate.
- HPP 9** Accurate – an organisation must take such steps as are reasonable in the circumstances to ensure that health information is relevant, accurate, up to date, complete and not misleading before using it.

## Use

- HPP 10** Limited use – an organisation must not use health information for a purpose other than the purpose for which it was collected unless the person consents to such use, the other purpose is a directly related purpose for which the person would reasonably expect the organisation to use the information. Otherwise, you generally need their consent.

## Disclosure

- HPP 11** Limited disclosure – only disclose health information for the purpose for which it was collected, or a directly related purpose that the person would expect. Otherwise, you generally need their consent.

## Identifiers & Anonymity

- HPP 12** Not identified – only identify people by using unique identifiers if it is reasonably necessary to carry out your functions efficiently.
- HPP 13** Anonymous – give people the option of receiving services from you anonymously, where this is lawful and practicable.

## Transferrals & Linkage

- HPP 14** Controlled – only transfer health information outside New South Wales in accordance with HPP 14.
- HPP 15** Authorised – people must expressly consent to participate in any system that links health records across more than one organisation. Only include health information about them, or disclose their identifier for the purpose of the health records linkage system if they have expressly consented to this.

Please note that the Department of Corrective Services falls within the definition of a “law enforcement agency” in section 4 of the HRIP Act. HPPs 10 and 11 contain exemptions from the operation of those principles for law enforcement agencies.

## **Exemptions to the Health Privacy Principles**

6.2 There are five sources of exemptions to the HRIP Act:

1. Exemptions written in the HRIP Act itself
2. Statutory guidelines issued under section 64 of the HRIP Act
3. Exemptions written in a health records and information privacy code of practice, made by the Attorney General under the HRIP Act
4. Exemptions written in a public interest direction, made by the privacy commissioner under section 62 of the HRIP Act
5. Exemptions written in a regulation made by the Attorney General under the HRIP Act.

## **Exemptions written in the HRIP Act**

6.3 Several exemptions to the HPPs are included in the HRIP Act. Those pertinent to the Department are as follows:

6.4 Section 19 provides that HPP 1 – HPP 4, HPP 7, HPP 8, HPP 13 and HPP 15 only apply to health information collected by the Department after the commencement of Schedule 1. The commencement date of Schedule 1 is 1 September 2004.

6.5 Clause 4(4) of Schedule 1 provides that an organisation is not required to comply with HPP 4 if the individual has expressly consented to the organisation not complying with it, or the information is collected for a law enforcement purpose.

6.6 Clause 10(1) of Schedule 1 provides in the following subclauses, that the Department must not use the health information it holds for a purpose other than the purposes for which it was collected unless:

- (a) The individual has consented to the use of the information for the secondary purpose, or
- (b) It is directly related to the primary purpose and the individual would reasonably expect the organisation to use it for that purpose, or
- (c) The use of the information is reasonably necessary to lessen or prevent:
  - (i) a serious and imminent threat to the life, health or safety of the individual or another person, or
  - (ii) a serious threat to public health or public safety, or
- (d) The use of the information is reasonably necessary for the funding, management, planning or evaluation of health services, or

- (e) The use of the information is reasonably necessary for the training of employees, or
- (f) The use of the information is reasonably necessary for research, or the compilation or analysis of statistics, in the public interest, or
- (h) The organisation has reasonable grounds to suspect that unlawful activity, unsatisfactory professional conduct or breach of discipline has been or may be engaged in, or
- (i) The use of the information is reasonably necessary for the exercise of law enforcement functions by law enforcement agencies in circumstances where there are reasonable grounds to believe that an offence may have been, or may be, committed, or
- (k) The use of the information is in the circumstances prescribed by the regulations for the purposes of this paragraph.

6.7 Clause 10(2) of Schedule 1 provides that an organisation is not required to comply with a provision of this clause if:

- (a) the organisation is lawfully authorised or required not to comply with the provision concerned, or
- (b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*).

6.8 Clause 11(1) of Schedule 1 provides in the following relevant subclauses that the Department must not disclose the health information it holds for a purpose other than the purposes for which it was collected unless:

- (a) The individual has consented to the disclosure of the information for that secondary purpose, or
- (b) It is directly related to the primary purpose and the individual would reasonably expect the organisation to disclose it for that purpose, or
- (c) The disclosure of the information is reasonably believed by the organisation to be necessary to lessen or prevent:
  - (i) a serious and imminent threat to the life, health or safety of the individual or another person, or
  - (ii) a serious threat to public health or public safety, or
- (d) The disclosure of the information is reasonably necessary for the funding, management, planning or evaluation of health services, or
- (e) The disclosure of the information is reasonably necessary for the training of employees, or
- (f) The disclosure of the information is reasonably necessary for research, or the compilation or analysis of statistics, in the public interest, or

- (g) The disclosure of the information is to provide the information to an immediate family member of the individual for compassionate reasons, or
- (i) The organisation has reasonable grounds to suspect that unlawful activity, unsatisfactory professional conduct or breach of discipline has been or may be engaged in, or
- (j) The disclosure of the information is reasonably necessary for the exercise of law enforcement functions by law enforcement agencies in circumstances where there are reasonable grounds to believe that an offence may have been, or may be, committed, or
- (l) The disclosure of the information is in the circumstances prescribed by the regulations for the purposes of this paragraph.

6.9 Clause 11(2) of Schedule 1 provides that an organisation is not required to comply with a provision of this clause if:

- (a) the organisation is lawfully authorised or required not to comply with the provision concerned, or
- (b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*).

6.10 Clause 14 of Schedule 1 provides in the following relevant subclauses that the Department must not transfer health information to any person or body who is in a jurisdiction outside New South Wales or to a Commonwealth agency unless:

- (a) the Department reasonably believes that the recipient of the information is subject to a law, binding scheme or contract that effectively upholds principles for fair handling of the information that are substantially similar to the Health Privacy Principles, or
- (b) the individual consents to the transfer, or
- (c) the transfer is necessary for the performance of a contract between the individual and the organisation, or
- (d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party, or
- (e) all of the following apply:
  - (i) the transfer is for the benefit of the individual,
  - (ii) it is impracticable to obtain the consent of the individual to that transfer,
  - (iii) if it were practicable to obtain such consent, the individual would be likely to give it, or
- (f) the transfer is reasonably believed by the organisation to be necessary to lessen or prevent:
  - (i) a serious and imminent threat to the life, health or safety of the individual or another person, or

- (ii) a serious threat to public health or public safety, or
- (g) the Department 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, or
- (h) the transfer is permitted or required by an Act (including an Act of the Commonwealth) or any other law.

6.11 Clause 15 of Schedule 1 provides that an organisation is not required to comply with a provision of this clause if:

- (a) the organisation is lawfully authorised or required not to comply with the provision concerned, or
- (b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*), or
- (c) the inclusion of health information about the individual in the health records information system is a use of the information that complies with HPP 10(1)(f) or a disclosure of the information that complies with HPP 11(1)(f).

### **Statutory guidelines issued under the HRIP Act**

6.12 The Privacy Commissioner may issue statutory guidelines under section 64 of the HRIP Act for or with respect to any matter for which guidelines may be issued under the HRIP Act. In particular the Privacy Commissioner may issue statutory guidelines for the purposes of HPP 3, 4, 10 and 11. They are legally binding documents that define the scope of particular exemptions in the HPPs. They describe how the exemption applies and what must be done to comply with the exemption. They are as important as the exemption itself. Currently, four guidelines have been issued which relate to the Department:

- use or disclosure of health information for the management of health services,
- use or disclosure of health information for training purposes,
- use or disclosure of health information for research purposes, and
- notification when collecting health information about a person from someone else.

6.13 Privacy NSW Fact sheet – No 3, November 2003, which provides information on the guidelines, advises that organisations seeking to rely on either the “management of health services” exemption in HPP 10(1)(b) and HPP 11(1)(b), the “training purposes” exemption in HPP 10(1)(e) or HPP 11(1)(e), the “research purposes” exemption in HPP 10(1)(f) and HPP 11(1)(f), or the “notification exemption” in HPP4(3) must do so in accordance with the relevant statutory guideline. Failure to comply with the statutory guidelines constitutes a breach of the HPPs and the HRIP Act.

6.14 The ‘Handbook to Health Privacy’ published by Privacy NSW provides Privacy NSW’s interpretation of the HRIP Act and may be viewed on the Privacy NSW website at:

[http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll\\_pnsw.nsf/pages/PNSW\\_03\\_hrphdbkindex](http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_03_hrphdbkindex)

The Statutory guidelines issued by the Privacy Commissioner may be viewed on the Privacy

NSW website at:

[http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll\\_pnsw.nsf/pages/PNSW\\_03\\_hripact#4b](http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_03_hripact#4b)

The Privacy NSW Fact sheet – No 3, November 2003 may also be viewed on the Privacy NSW website at:

[http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll\\_pnsw.nsf/vwFiles/FS3\\_HRIPA.pdf/\\$file/FS3\\_HRIPA.pdf#target='\\_blank'](http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/vwFiles/FS3_HRIPA.pdf/$file/FS3_HRIPA.pdf#target='_blank')

## Health Records and Information Privacy Codes of Practice

- 6.15 Health privacy codes of practice which modify the application of the health privacy principles or the Part 4 access provisions of the HRIP Act may be made under Part 5 of the HRIP Act. Currently one code, the *Health Records and Information Privacy Code of Practice 2005* (health code) has been made which is applicable to human services agencies.

The Department of Premier and Cabinet had deemed this Department to be a justice agency and not a human services agency. The types of health services listed in section 4(1) of the health code are not this Department's core business. Notwithstanding, for the purposes of the NSW Housing and Human Services Accord, references to human services explicitly include the Department's Community Offender Services.

## Exemptions provided by section 62 directions

- 6.16 Under section 62 of the HRIP Act, the Privacy Commissioner may make a written direction that an organisation is not required to comply with an HPP, a provision of Part 4 of the HRIP Act or a health privacy code of practice, or that the application of an HPP, a provision of Part 4 or a code to an organisation is to be modified as specified in the direction.
- 6.17 Currently the following section 62 directions are applicable to the Department:
- Direction relating to the Anti-Social Behaviour Pilot Project
  - Direction relating to the Redfern Waterloo Partnership Project.

Section 62 directions may be viewed on Privacy NSW's website at:

[http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll\\_pnsw.nsf/pages/PNSW\\_03\\_hrippid#3](http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_03_hrippid#3)

## Exemptions written in a regulation made under the HRIP Act

- 6.18 The *Health Records and Information Privacy Regulation 2006* makes exemptions in relation to the electronic health records pilot program conducted by the Department of Health. There is also reference to the Aboriginal Trust Funds Repayment Scheme (ATFRS) exemption. A public sector agency is exempt from clauses 10 and 11 of Schedule 1 in respect of a disclosure of health information to an ATFRS agency (Department of Aboriginal Affairs, the State Records NSW or the Department of Premier and Cabinet) in connection with the implementation and operation of the ATFRS.

## **Corrupt disclosure and use of health information by public sector officials and other offences**

- 6.19 Section 68 of the HRIP Act provides that intentional disclosure or use of health information by public sector officials is an offence punishable by up to 100 penalty units or two years imprisonment, or both.
- 6.20 Section 69 of the HRIP Act provides that a person who offers to supply (whether to a particular person or otherwise), or holds himself or herself out as being able to supply (whether to a particular person or otherwise), health information that the person knows, or ought reasonably to know, has been or is proposed to be disclosed in contravention of section 68 is guilty of an offence punishable by up to 100 penalty units or two years imprisonment, or both.
- 6.21 Section 70(1) of the HRIP Act provides that a person must not, by threat, intimidation or misrepresentation, persuade or attempt to persuade an individual:
- (a) to refrain from making or pursuing:
    - (i) a request for access to health information, or
    - (ii) a complaint to the Privacy Commissioner or the Tribunal under Part 6, or
    - (iii) an application under Part 5 of the PPIP Act with respect to the alleged contravention of a Health Privacy Principle or a health privacy code of practice, or
  - (b) to withdraw such a request, complaint or application.
- 6.22 Section 70(2) further provides that a person must not, by threat, intimidation or false representation, require another person:
- (a) to give a consent under this Act, or
  - (b) to do, without consent, an act for which consent is required.

Offences under section 70 are punishable by fines of up to 100 penalty units.

## **Access to and amendment of health information**

- 6.23 The Department has prepared a paper entitled, *Public Access to Records, Documents, Personal Information and Health information*. The paper, among other things, explains how health information held by the Department, or held on behalf of the Department by State Records NSW, may be obtained. The paper is available on the Department's intranet and Internet sites.
- 6.24 Under section 16 of the FOI Act you have the right to apply to the Department for access to any documents held by it about you. Under section 39 of the FOI Act you may apply to the Department to have any document held by it about you amended if you consider that the information contained in the document is incomplete, incorrect, out of date or misleading.

6.25 Section 22(3) of the HRIP Act provides:

“Without limiting the generality of subsection (1), the provisions of the FOI Act that impose conditions or limitations (however expressed) with respect to any matter referred to in HPP 6 (Information about health information held by organisations), HPP 7 (Access to health information) or HPP 8 (Amendment of health information) are not affected by this Act, and those provisions continue to apply in relation to any such matter as if those provisions were part of this Act.”

Accordingly any request made pursuant to HPPs 6, 7 and 8, will be largely processed as if it had been made under the FOI Act; however, the appeal rights differ.

6.26 For details on how to make an application under the FOI Act, contact the FOI & Privacy Unit on 8346 1359 or refer to the Department’s Internet site: [www.dcs.nsw.gov.au](http://www.dcs.nsw.gov.au).

Section 22 of the HRIP Act states:

**“22 Freedom of Information Act 1989 not affected**

- (1) Nothing in this Act affects the operation of the *Freedom of Information Act 1989*.
- (2) In particular, this Act does not operate:
  - (a) to modify any exemption under the *Freedom of Information Act 1989*, or
  - (b) to lessen any obligations under that Act in respect of a public sector agency.”

## **7. Disclosure of Departmental information to other government agencies**

- 7.1 The Department will disclose specified information to other government agencies, if the other agency has legislative authority, to obtain the specified information.
- 7.2 Agencies, such as NSW Police, Department of Housing or Centrelink for example, may require information held by the Department in order to carry out their functions. These requests must be in writing and addressed to a relevant officer of the Department. The request must be written on the agency's letterhead and quote the relevant legislation that the agency is relying on in order to obtain the information.
- 7.3 The information provided regarding the legislative authority is checked by a Departmental officer to ensure that the outside agency has the authority it claims in order to obtain the information.
- 7.4 The written request must be kept in the Department's corporate records for any necessary future reference.
- 7.5 Disclosure of personal information is also covered by section 16 of Part 5 of the *Privacy Code of Practice (General) 2003* which allows the Department to divert from sections 18 and 19 (IPPs 11 and 12) of the PPIP Act, if non-compliance is reasonably necessary to enable the Department to protect the safety, welfare or well-being of a person; to provide services and programs to an offender effectively; to permit the Department of Community Services, the Department of Health or JH to exercise its functions properly; or to disclose personal information to a person for the purposes of an investigation, but only if the disclosure is made to a person to verify the information, or to obtain professional or technical advice about the information.

## 8. Disclosure of information with government agencies and non-government organisations

- 8.1 In order to provide certain services and programs to satisfy requirements of the State Plan, including those of the NSW Housing and Human Services Accord (Accord), it is necessary to share information (disclose information) across participating government agencies and non-government organisations.
- 8.2 The Department may provide information to the Department of Housing, Wesley Mission, ARTD Pty. Ltd., the Community Restorative Centre and other signatory agencies, in order to provide support services under the Accord.
- 8.3 A client information sharing agreement has been developed between the signatory agencies and non-government organisations of the Accord.
- 8.4 As the Accord explicitly includes the Department's Community Offender Services as a human services agency, the collection, use and disclosure of personal information is also covered by Part 4 of the *Privacy Code of Practice (General) 2003* (Part 4 of Code). Section 10(2) of Part 4 of the Code, states that "despite the information protection principles, a human services agency may collect and use personal information about an individual to another human services agency or an allied agency, if the collection, use or disclosure is in accordance with a written authorisation given by a senior officer of the agency.
- 8.5 Disclosure of personal information is also covered by section 16 of Part 5 of the *Privacy Code of Practice (General) 2003* which allows the Department to divert from sections 18 and 19 (IPPs 11 and 12) of the PPIP Act, if non-compliance is reasonably necessary to enable the Department to protect the safety, welfare or well-being of a person; to provide services and programs to an offender effectively; to permit the Department of Community Services, the Department of Health or JH to exercise its functions properly; or to disclose personal information to a person for the purposes of an investigation, but only if the disclosure is made to a person to verify the information, or to obtain professional or technical advice about the information.

## 9. The *Crimes (Administration of Sentences) Act 1999* and other legislation affecting information held by the Department of Corrective Services

9.1 Although the PPIP Act and the HRIP Act are the primary laws that regulate the collection, holding, use and disclosure of personal and health information, there are many other laws which affect how the Department deals with such information. Those laws (excluding codes of practice, section 41 and section 62 directions and regulations made under the PPIP Act and the HRIP Act) are discussed in this section. The excluded legislation is discussed in sections 5 and 6 of this Plan.

### Crimes (Administration of Sentences) Act 1999

9.2 The major piece of non-privacy legislation affecting the handling of personal and health information by the Department is the *Crimes (Administration of Sentences) Act 1999* (Act) and the regulations made under that Act. The major provisions of the Act, and the regulation made under it, concerning personal and health information are set out in the tables below.

#### Relevant provisions of the *Crimes (Administration of Sentences) Act 1999*

Section	Provision
42 to 46	It is the duty of the General Manager of a correctional centre, or any other officer doing duty at a correctional centre, to accept the custody of any prisoners who are liable to undergo imprisonment or other detention in custody under a law in force in the Australian Capital Territory. Likewise, a General Manager must deliver the prisoner into the custody of a constable who presents an Australian Capital Territory warrant for the delivery or the conveyance of the prisoner to the Australian Capital Territory.
67(1)	When the SORC proposes to recommend a low security classification for a serious offender, the SORC is (subject to and in accordance with the regulations) required to give a preliminary notice of its intention to any victim of the offender whose name is recorded in the Victims' Register.
106Y(1)	Section 106Y applies to such persons as are prescribed by the regulations for the purposes of this section, being persons who are involved in the administration of, or who provide services in connection with, an offender's drug treatment under Part 4A of the Act.
106Y(3)(b)	The provision of any information (protected information) relating to an offender that is provided to the Drug Court or the Commissioner, or to any person prescribed by the regulations for the purposes of this section, by a person prescribed by the regulations, does not constitute a contravention of the HRIP Act or the PPIP Act. Clause 201C of the <i>Crimes (Administration of Sentences) Regulation 2001</i> prescribes certain persons for the purposes of section 106Y.
106Y(5)	An offender is taken to have authorised the communication of protected information: <ul style="list-style-type: none"> <li>(a) from any person to whom section 106Y applies to the registrar of the Drug Court or the Commissioner, and</li> <li>(b) from the registrar of the Drug Court or the Commissioner to any person to whom section 106Y applies, and</li> <li>(c) from any member of staff of the Drug Court or the Department to any</li> </ul>

	other member of staff of the Drug Court or the Department.
106Y(6)	A provision of any Act or law that prohibits or restricts the disclosure of information does not operate to prevent the provision of information in accordance with section 106Y.
139(3)	A notice given under section 139(1): (a) must indicate the address to which such an application should be sent, and the date by which such an application must be made, and (b) subject to section 194, must be accompanied by copies of the reports and other documents intended to be used by the State Parole Authority (SPA) in making its final decision.
145(1)	As soon as practicable after forming an initial intention to make a parole order for a serious offender, but subject to and in accordance with the regulations, SPA must give notice of its intention to those victims of the offender (if any) whose names are recorded in the Victims' Register.
146(3)	A notice to offender of decision to refuse bail, given under section 146(1): (a) must indicate the address to which such an application should be sent, and the date by which such an application must be made, and (b) subject to section 194, must be accompanied by copies of the reports and other documents intended to be used by SPA in making its final decision.
165AA(1)	On referring an offender for assessment in relation to the making of a home detention order under section 165, SPA may make a temporary release order releasing the offender from custody or permitting the offender to remain at large, subject to such supervision as is prescribed by the regulations, pending SPA's decision as to whether or not to make the home detention order. Clause 226(2)(d) of the regulations provides that as part of the supervision, the offender is to authorise his or hers medical practitioners, their therapist (if any) and their counsellor (if any) to provide information about him or her to the offender's probation and parole officer.
173(2)(d)	A revocation notice issued under section 173(1) must be accompanied by: (i) a copy of the revocation order by which the periodic detention order, home detention order or parole order was revoked, and (ii) copies of the reports and other documents used by SPA in making the decision to revoke the periodic detention order, home detention order or parole order and, if appropriate, the decision to specify the earlier day.
193A(2)	Subject to section 194, a victim of a serious offender is entitled to be given access to all documents held by or on behalf of SPA in relation to the offender, but only to the extent to which those documents indicate the measures that the offender has taken, or is taking, to address his or her offending behaviour.
194	(1) Nothing in this Act or the regulations requires a person to be provided with a copy of a report or another document (or any part of the report or document) if its provision to the person may, in the opinion of a judicial member of SPA: (a) adversely affect the security, discipline or good order of a correctional centre, or (b) endanger the person or any other person, or (c) jeopardise the conduct of any lawful investigation, or (d) prejudice the public interest, or (e) adversely affect the supervision of any offender who has been released

	<p>on parole, or</p> <p>(f) disclose the contents of any offender's medical, psychiatric or psychological report.</p> <p>(2) Subsection (1) does not permit the Minister to be denied access to any document held by SPA.</p>
197	Sections 197(2)(b) and 197(2)(c) provides for reports from SORC to be provided to the Supreme Court and SPA.
209A	A report or another document held by the SORC is not to be provided to a person if, in the opinion of a judicial member, certain circumstances apply.
236B	The Chief Executive of JH is to have free and unfettered access to all medical records held at a correctional centre for the purposes of ensuring compliance with the provisions of the Act and the regulations at a correctional centre.
244	The Chief Executive of JH is to have free and unfettered access to all medical records held at a managed correctional centre for the purposes of ensuring compliance with the provisions of the Act and the regulations at a managed correctional centre.
247	<p>While a correctional centre is being managed under a management or submanagement agreement, the <i>Freedom of Information Act 1989</i> and the regulations under that Act apply, with any necessary modifications, to and in respect of the management company or submanagement company and its members and employees:</p> <p>(a) as if the management company or submanagement company (in so far as it has functions under this Act or the agreement) were a local authority within the meaning of that Act, and</p> <p>(b) as if the managing director of the management company or submanagement company were its principal officer within the meaning of that Act, and</p> <p>(c) as if the Minister were its responsible Minister within the meaning of that Act.</p>
256(2)	Section 256(2) provides that the Victims' Register is to record the "names of victims of offenders who have requested that they be given notice of the possible parole of the offender concerned".
257	<p>A person must not disclose any information obtained in connection with the administration or execution of this Act unless that disclosure is made:</p> <p>(a) with the consent of the person from whom the information was obtained, or</p> <p>(b) in connection with the administration or execution of this Act, or</p> <p>(c) for the purposes of any legal proceedings, or</p> <p>(d) in accordance with a requirement of the Ombudsman Act 1974, or</p> <p>(e) with other lawful excuse.</p>
267(2)	A person must apply to the Commissioner of Corrective Services for approval to conduct research that involves the person (or persons acting under the direction of that person) obtaining access to departmental information.

**Relevant provisions of the *Crimes (Administration of Sentences) Regulation 2001***

Clause	Provision
5(1)	The General Manager of a correctional centre must record such of the information as set out in Schedule 1 of the regulation as is relevant to the inmate. The General Manager is also to record such other information as the Commissioner considers appropriate to be recorded.
12	A case management plan is to be prepared and adopted for each inmate in a correctional centre.
13	The case management plan will include details such as the provision of services and programs including health care. The information to prepare the plan will be obtained from sentencing court's comments, any physical and mental health assessments, criminal history and other information.
80	The General Manager of a correctional centre must record certain particulars concerning all visitors to inmates. Copies of the record are to be kept in such manner and for such period as the Commissioner determines.
93(1)	An authorised officer may require a visitor to submit to an inspection and search of personal possessions, scanning by means of an electronic scanning device and to be sniffed by a dog. A visitor may also be required to empty their pockets and allow an inspection and search of any vehicle under their control on the premises of a correctional centre.
109	The General Manager of a correctional centre or a nominated officer may open, inspect and read a letter or parcel sent to or by an inmate and, if it contains prohibited goods, may confiscate the letter or parcel and its contents and deal with them in accordance with the directions of the Commissioner. The inmate is to be informed of the confiscation of any letter, parcel or prohibited goods. A nominated officer may direct that any written or pictorial matter contained in a letter or parcel opened, inspected or read under this clause be copied before the letter or parcel containing the matter is delivered to the addressee, if the nominated officer is of the opinion that the written or pictorial matter to be copied contains anything likely to prejudice the good order and security of any correctional centre, or is threatening, offensive, indecent, obscene or abusive. This clause does not apply to any letter or parcel addressed to, or received from, an exempt body or exempt person, or any letter or parcel to which clause 110A applies.
110A	The General Manager of a correctional centre or a nominated officer may open, inspect and read a letter or parcel sent to or by a Category AA male inmate or Category 5 female inmate and, if it contains prohibited goods, may confiscate the letter or parcel and its contents and deal with them in accordance with the directions of the Commissioner. There is no requirement for the inmate to be informed of the confiscation of any letter, parcel or prohibited goods. Letters or parcels sent to or from exempt bodies or persons are not to be opened by correctional centre officers. A register must be kept for each correctional centre in which nominated officers are to record certain details, including personal information, with respect to each letter or parcel dealt with under this clause.
114	Where a nominated officer finds that a letter, parcel or other article contains information or any other thing that the officer has reasonable grounds to believe is likely to prejudice the good order and security of a correctional centre, or relates to a criminal offence which has been or may be committed,

	the officer must report the circumstances to the General Manager as soon as practicable. The General Manager of a correctional centre may furnish particulars of the information to a police officer or deliver the letter, parcel or article to a police officer.
151	The Commissioner may provide the results of positive urine tests to the Chief Executive Officer of JH and, in the case of tests on serious offenders, to SORC.
171	The functions of the Ethics Committee are as follows: (a) to consider applications for approval to undertake research and make recommendations to the Commissioner as to whether or not such applications should be approved and, if so, on what conditions, (b) to advise the Commissioner on the records and information that may be provided to persons undertaking research, as referred to in section 267 of the Act, and the conditions on which any such records and information are to be so provided, (c) to advise the Commissioner on the conditions on which such a person may be issued with a visitor's permit under Division 3 of Part 4 of this Chapter, (c1) to advise the Commissioner on ethical issues, (d) to advise the Commissioner on such other matters as the Commissioner may refer to the Committee for advice.
174	A correctional officer may search a periodic detainee each time they report for detention and at other times as appropriate. The search must not be conducted in the presence of a person of the opposite sex, except in an emergency. The search must be conducted with due regard to dignity and self-respect. A periodic detainee must not resist or impede the conduct of such a search (as this would be an offence against discipline).
201D	The Commissioner is to ensure that each offender is to undergo periodic drug testing. An authorised person may in accordance with the Commissioner's instructions collect a sample of one or more of the following: (a) breath (b) urine (c) oral fluid (d) hair
201E	This clause provides for random drug testing of offenders.
226(2)(d)	The offender is to authorise the following persons to provide information about him or her to the officer: (i) the offender's medical practitioners, (ii) the offender's therapist (if any), (iii) the offender's counsellor (if any)
236	This clause provides that a correctional officer must give written notice to the Commissioner as to any offender to whom the officer is related or is an associate.
240	The General Manager may request Departmental officers to submit to an inspection and search of personal possession, scanning by electronic scanning device and to be sniffed by a dog. Officers may also be required to empty their pockets and make available for inspection any room, locker or vehicle that is under the officer's control at the centre.
249	This clause provides that a person involved in the administration of the Act

	<p>is not authorised to furnish to any other person</p> <p>(a) a photograph, film or video or audio recording of an inmate, or</p> <p>(b) an impression of an inmate's handprints, fingerprints, footprints or toeprints, or</p> <p>(c) any other forensic material (within the meaning of the <i>Crimes (Forensic Procedures) Act 2000</i>) relating to an inmate.</p> <p>Clause 249 does not apply in the circumstances referred to in section 257 (a)–(e) of the Act.</p>
249AB	<p>A person must not interfere or tamper with, or destroy, a sample of blood or a non-invasive sample provided by or taken from a member of correctional staff under Division 5 of Part 11 of the Act unless the sample is destroyed:</p> <p>(a) by or at the direction of an analyst in the course of or on completion of analysis, or</p> <p>(b) in the case of a sample handed to a person on behalf of a member of correctional staff, by or at the direction of the person, or</p> <p>(c) after the expiration of 12 months commencing on the day on which the sample was taken or provided, or a longer period (being no more than 5 years) as directed by the Commissioner in respect of the sample in a direction made before such an expiration.</p>
251	<p>A prescribed JH officer must, as soon as practicable after forming an opinion about the physical and mental well-being of an inmate, report that he or she has formed such an opinion to a prescribed Department of Corrective Services officer.</p>
252	<p>In the case of a serious offender, clause 252 requires the prescribed officer to send written notice of the report about the mental state of the serious offender to SORC.</p>
253	<p>A prescribed JH officer must report to a prescribed Departmental officer, his or her opinion that an inmate's diet, exercise or other treatment should be varied or modified for reasons of health. In the case of a serious offender, clause 253 requires the prescribed Corrective Services officer to send written notice of the report about the diet, exercise or other treatment of the serious offender to the SORC.</p>
254	<p>Proper medical records are to be kept in respect of each inmate in the custody of a prescribed JH officer, and their contents are not to be divulged to any person outside JH (including the inmate) except in accordance with guidelines established by the Chief Executive Officer, JH. This does not prevent information in an inmate's medical records from being used to prepare general reports on the inmate's health for submission to the General Manager of a correctional centre, and such a report must be prepared and submitted whenever the General Manager so requests.</p>
256	<p>This clause requires a prescribed JH officer to report his or her opinion that an inmate has, or appears to have, a serious infectious disease, to a prescribed Department of Corrective Services officer.</p>
257	<p>This clause requires a prescribed JH officer, on becoming aware that an inmate has died, must report the death to the Commissioner.</p>
280(1)	<p>The General Manager of a correctional centre must ensure that a record is kept at the correctional centre of each correctional officer, Departmental officer, medical officer or nursing officer employed within the centre, certain information concerning inmates and such other information as the Commissioner may require a record to be kept.</p>
285	<p>(1) The Commissioner is to ensure that the following requirements are complied with in relation to the operation of an authorised biometric</p>

	<p>identification system in any correctional centre:</p> <p>(a) the fingerprint image of any person must not be retained on the system, and must be deleted as soon as the person's biometric algorithm is made,</p> <p>(b) a person's biometric algorithm must not be made, stored or kept as part of any other database that is maintained by or on behalf of the Department,</p> <p>(c) the system must not be used to reconstruct a fingerprint pattern from a person's biometric algorithm,</p> <p>(d) the photo image of each visitor to a correctional centre must be eliminated from the system:</p> <p>(i) within 6 months of the person's last recorded visit to a correctional centre, or</p> <p>(ii) as soon as possible at the request of the person,</p> <p>(e) a person's biometric algorithm must not be stored in the system's database in such a way that would enable unauthorised access to the information,</p> <p>(f) permission must not be given to any person or agency that would enable any person (other than a correctional officer or Departmental officer) to gain access to a person's biometric algorithm stored in the system's database.</p> <p>(2) Any person who is involved in the operation of an authorised biometric identification system must not knowingly or negligently:</p> <p>(a) permit any person to gain access to any information in the system's database, or</p> <p>(b) provide such a person with any information in the system's database, or</p> <p>(c) use the system to reconstruct a person's fingerprint pattern from the person's biometric algorithm.</p> <p>This clause does not prevent access to a person's photo image or personal details from being given to the Commissioner, the principal officer (however described) of a law enforcement agency, or any other person or agency for a lawful purpose.</p>
287(2)	<p>Subject to certain exceptions in clause 287(3), a person who communicates directly or indirectly any information that has been included in the Victims' Register, or that has been disclosed so that it may be included in that Register, and knows that the information has been so included or disclosed, is guilty of an offence.</p>

## Other legislation

9.3 Other non-privacy legislation concerning personal and health information which affect the Department is set out below.

**Anti-Discrimination Act 1977** - authorises the collection of information necessary for the preparation of an equal opportunity management plan (which may include special classes of personal information referred to in section 19(1) of the PPIP Act).

**Bail Act 1978** – an Act, applying to a person whether or not the person has attained the age of 18 years, relating to bail for accused persons in or in connection with criminal proceedings.

**Child Protection (Offenders Prohibition Orders) Act 2004** – an Act with respect to orders prohibiting certain offenders who pose a risk to the lives or sexual safety of children from engaging

in specified conduct; and for other purposes.

**Child Protection (Offenders Registration) Act 2000** - section 6 requires the Department to give written notice to the Commissioner of Police when a registrable person:

- ceases to be in custody,
- ceases to be subject to a supervised sentence,
- ceases to participate in the Pre-Trial Diversion of Offenders Program,
- ceases to be subject to a condition of parole requiring the person to be subject to supervision, or
- ceases to be an existing licensee.

Section 21D of the *Child Protection (Offenders Registration) Act 2000* authorises government agencies to disclose information concerning a registrable person to the Commissioner of Police or a supervising authority. Clause 5(c) of the *Child Protection (Offenders Registration) Regulation 2001* includes the Commissioner of Corrective Services within the definition of supervising authority for the purposes of the Act.

**Children and Young Persons (Care and Protection) Act 1998** - section 248 authorises government agencies to exchange information as it relates to the wellbeing, care and protection of children.

**Coroners Act 1980** – an Act that requires notification to the Coroner of deaths occurring under certain conditions.

**Crimes Act 1900** - Part 6 of the *Crimes Act* creates offences for unauthorised obtaining of access to or interference with data in computers. There are higher penalties for accessing certain categories of sensitive government information eg law enforcement information or for alteration or destruction of data.

**Crimes (Forensic Procedures) Act 2000** - section 109 prohibits the disclosure of information stored on a DNA database system or any other information revealed by forensic procedure carried out on a suspect, offender or volunteer, except in the circumstances provided by the section. Intentional or reckless disclosure in contravention of the section is an offence. Clause 11 of the *Crimes (Forensic Procedures) Regulation 2000* provides that for the purposes of section 109(2)(g) of the Act, any purpose relating to the security classification, placement or management by or under the *Crimes (Administration of Sentences) Act 1999* of a classifiable person is a prescribed purpose for which a person may disclose information that relates to the classifiable person that is stored on the DNA database system. For the purposes of section 109(3)(o) of the Act, any purpose relating to the security classification, placement or management by or under the *Crimes (Administration of Sentences) Act 1999* of a classifiable person is a prescribed purpose for which a person may disclose information relating to the classifiable person revealed by the forensic procedure that was carried out on the classifiable person.

**Crimes (Interstate Transfer of Community Based Sentences) Act 2004** - section 15 provides that the Department may register an interstate sentence in NSW at the request of an interstate authority for that interstate jurisdiction in which the sentence is in force. Section 16 requires the request to include certain kinds of personal information about the offender. Clause 1 of Schedule 1 of the *Crimes (Interstate Transfer of Community Based Sentences) Regulation 2004* sets out the personal information required to be entered in the local register for the registration of an interstate sentence.

Section 25 of the *Crimes (Interstate Transfer of Community Based Sentences) Act 2004* provides

that the Department may request an interstate authority for an interstate jurisdiction to register a local sentence in the interstate jurisdiction. Section 26 provides that the Department may, at the request of the interstate authority or on its own initiative, give the interstate authority any additional information about the local sentence or the offender.

**Crimes (Sentencing Procedure) Act 1999** – An Act which lists the different types of sentences that may be issued and includes sections on assessments and reports that may be created and used to assist in sentencing an individual.

**Criminal Records Act 1991** - restricts access to and disclosure of spent and quashed convictions. Bureau of Crime Statistics and Research (BOCSAR) and the Director of Public Prosecutions are exempted from restrictions on disclosure.

**Criminal Records Regulation 2004** - Clause 13 provides that for the purposes of section 13 of the *Criminal Records Act 1991*, information may be disclosed by the officer in charge of the Criminal Records Section of NSW Police to a person employed in the Department under certain circumstances.

**Fines Act 1996** - authorises and requires the Department to provide the State Debt Recovery Office, on request, with available information about the criminal record, address or assets of a fine defaulter for the purposes of the Office taking action against the person to enforce payment of a fine.

**Freedom of Information Act 1989** - deals with applications for access to documents which may contain personal information and applications for amendment of operational records of information relating to the personal affairs of the applicant. The Act creates an alternative means of accessing personal and health information. The Department may use limitations and conditions affecting access under the FOI Act when responding to requests for access made under the PPIP Act and the HRIP Act. When FOI applicants seek access to documents that contain information concerning the personal affairs of third-parties, consultation with those third-parties is required before the Department may consider releasing the documents.

**Health Administration Act 1982** – Section 22 refers to disclosure of information without the consent of the individual to be an offence.

**Health Services Act 1997** – This Act lists some of the key functions to include the provision of health care and makes reference to collection, use and disclosure of information to comply with HPPs 1, 10 and 11.

**Independent Commission Against Corruption Act 1988** - defines corrupt conduct in a way, which has been found to relate to unauthorised disclosures of information for personal benefit.

**Industrial Relations Act 1996** – During industrial consultation, personal and health information may be provided to authorised representatives. Where there is a suspected breach of the *Industrial Relations Act*, an authorised representative of an industrial organisation may view any employee's records and other documents kept by the employer that relate to the suspected breach. Copies may also be made of such records at that time.

**International Transfer of Prisoners (New South Wales) Act 1997** - gives effect to the scheme for the international transfer of prisoners set out in the *International Transfer of Prisoners Act 1997* (Cth) by enabling such prisoners to be transferred to and from New South Wales. When these prisoners become inmates in the NSW correctional system, they are subject to the NSW and

Commonwealth laws pertaining to them, including privacy and other laws listed here.

**International Transfer of Prisoners Act 1997 (Cth)** - in conjunction with its counterpart in NSW law, namely the *International Transfer of Prisoners (New South Wales) Act 1997*, creates a scheme by which international prisoners may be transferred to and from the NSW correctional system. When these prisoners become NSW inmates, they are subject to the NSW and Commonwealth laws pertaining to them, including privacy and other laws listed here.

**Listening Devices Act 1984** - section 5 prohibits the use of listening devices to record or listen to a private conversation, subject to certain exceptions. Section 6 prohibits the communication or publishing of a private conversation, or a report of a private conversation, as a result, direct or indirect, of the use of a listening device in contravention of section 5, subject to certain exceptions.

**Migration Act 1958 (Commonwealth)** – Section 18 of this Act requires that upon written notification from the Minister, information must be provided within the defined period and in the manner specified.

**Occupational Health and Safety Act 2000** – During industrial consultation, personal and health information may be provided to authorised representatives. Where there is a suspected breach of the *Occupational Health and Safety Act*, an authorised representative of an industrial organisation may view any employee's records and other documents kept by the employer that relate to the suspected breach. Copies may also be made of such records at that time.

**Ombudsman Act 1974** – Section 18 of this Act requires that upon written request from the Ombudsman a public authority may be required to provide a statement of information, a copy of a document or thing in order for the Ombudsman to carry out investigations.

**Parole Orders (Transfer) Act 1983** - relates to the reciprocal enforcement of parole orders within New South Wales and within other States or any Territory of the Commonwealth. When the Minister for Justice requests that another State or Territory register a parole order, documents relevant to the parole order must accompany the request. Conversely when the Minister for Justice is requested by his or her counterpart in another State or Territory to register a parole order in NSW, the Minister will receive documents relevant to that request. In both cases, the way the Department of Corrective Services handles any personal information contained in those documents is subject to the PPIP Act and the HRIP Act.

**Prisoners (Interstate Transfer) Act 1982** - relates to the interstate transfer of prisoners. Where a prisoner is transferred interstate, documents relevant to the transfer and to the prisoner must be sent to the corresponding Minister of the participating State or Territory. Conversely when a prisoner is transferred to NSW from another State or Territory, documents relating to that prisoner will be sent to the Department of Corrective Services. In both cases the way the Department of Corrective Services handles any personal information contained in those documents is subject to the PPIP Act and the HRIP Act.

**Protected Disclosures Act 1994** - the definition of personal and health information under privacy legislation excludes information contained in a protected disclosure. This means that a person cannot seek review of the use or disclosure of a protected disclosure or be prosecuted for unauthorised disclosure of protected disclosure information under the PPIP or the HRIP Act.

**Public Finance and Audit Act 1983** – Division 2 refers to access to certain information in relation to public or other money and public or other property.

**Public Sector Employment and Management Act 2002** - provides that when an employee

of the Department becomes bankrupt, or makes a composition, arrangement or assignment for the benefit of his or her creditors, the employee must provide to the appropriate Department Head notice of the bankruptcy, composition, arrangement or assignment along with any information with respect to the cause of the bankruptcy or of the making of the composition, arrangement or assignment as that Department Head requires. Any personal information contained in the documents provided to the Department must be handled according to applicable provisions of the PPIP Act and the HRIP Act.

**Social Security (Administration) Act 1999 (Cth)** – Centrelink may request information under section 192 in relation to any social security payment or claim.

**State Records Act 1998** - defines the circumstances under which the Department can dispose of its records and authorises the State Records NSW to establish policies, standards and codes to ensure adequate records management by the Department.

**Summary Offences Act 1988** – This act makes reference to the powers of correctional officers to stop, detain, search, seize and arrest individuals and/or their possessions.

**Telecommunications (Interception and access) Act 1979 (Cth)** – prohibits the interception of, and other access to, telecommunications except where authorised in special circumstances or for the purpose of tracing the location of callers in emergencies, and for related purposes.

**Victims Support and Rehabilitation Act 1996** - authorises the Department to provide the Director, Victims Services, with information about the address of a defendant for the purpose of serving a provisional order for restitution on the defendant or taking any action against the defendant to enforce an order for restitution.

**Workplace Surveillance Act 2005** – Lawful surveillance of an employee is covered in Part 2, which sets out the notification requirements of workplace surveillance of employees. Surveillance of an employee that does not comply with Part 2 is deemed covert surveillance, which is an offence under the Act unless the surveillance is authorised by a covert surveillance authority (Part 4). Law enforcement, correctional centres, courts and casinos are exempted (section 21). Part 3 covers surveillance which is prohibited, eg. change rooms and bathrooms.

## **General Law**

Compliance with or exemption from the requirements in the PPIP Act and the HRIP Act will not necessarily affect obligations of the Department which arise under other legislation or under general law principles. There are obligations arising under general law principles of confidentiality, legal professional privilege, privilege for confidential professional communications (for example, psychologists) and public interest immunity which affect the way in which the Department collects, holds, uses and discloses personal and health information.

## 10. Service-wide policies or documents affecting personal or health information held by the Department of Corrective Services

- “Attorney General’s Guidelines on making access directions under Part 6 of the *State Records Act 1998*”
- “Consultancy Agreement” developed by Crown Solicitor’s Office of New South Wales
- Department of Premier and Cabinet’s “Policy and Guidelines on Alcohol and other Drugs”
- Department of Premier and Cabinet’s Circular C2007-27 “Privacy Guidelines on Disclosure of Information during Industrial Relations Consultations”
- “NSW FOI Manual” – a joint publication of NSW Department of Premier and Cabinet and the NSW Ombudsman, August 2007
- NSW Ombudsman’s “FOI policies and guidelines (2<sup>nd</sup> edition)”
- NSW Ombudsman’s “Good Conduct and Administrative Practice” guidelines for state and local government (2<sup>nd</sup> edition)
- “NSW Police Service External Client ‘on-line’ Access Policy”
- “Policy and Guidelines for the use by Staff of Employer Communication Devices”
- “Protocol for Acceptable use of Internet and Electronic Mail”
- “The Personnel Handbook” prepared by the Department of Premier and Cabinet

## 11. Departmental policies or documents affecting personal or health information held by the Department of Corrective Services

- Access Direction 303 – “Records relating to individual offenders and staff”
- ACO 96/127 – “Provision of information concerning inmates and ex-inmates”
- ACO 97/101 – “Appropriate documentation on files”
- ACO 98/029 – “Offender management system – missing data”
- “Code of Conduct and Ethics 2005”
- Commissioner’s Instruction 03/2002 – “Association with Offenders”
- Commissioner’s Instruction 04/2002 – “Personal relationships with offenders”
- Commissioner’s Instruction 07/2002 – “Misleading Statements and Official Documentation”
- Commissioner’s Instruction 03/2003 – “Preparation of Reports on Offenders”
- Commissioner’s Instruction 09/2005 – “Management of Requests by NSW Police for Information Pursuant to section 16 of the *Child Protection (Offenders Prohibition Orders) Act 2004*”
- Commissioner’s Instruction 03/2005 – “Requests for Exchange of Information from the Department of Community Services”
- Commissioner’s Memorandum 04/25 – “Unauthorised Disclosure of Personal Information”
- Commissioner’s Memorandum 2005/28 – “Information Security Policy”
- Commissioner’s Memorandum 2006/22 – “Processing Visitor details onto OIMS”
- Commissioner’s Memorandum 2007/40 – “OIMS case notes”
- “Corporate Records Management Procedures Manual”
- “DCS Online” policy
- “FOI & Privacy Unit Proof of Identity” policy
- “IC&T Electronic Mail” policy
- “Information Security” policy (In particular see section 5, Authorised Use of IT.)
- “IC&T Information Classification and Ownership” policy
- Information Management procedure – “Family History and Research Requests”
- “Inmate Classification and Case Management Procedures Manual”
- Memoranda of Understanding (MOU) with other organisations involving the exchange of personal information. Agencies with which the Department has MOUs include TAFE, BOCSAR, JH, Tresillian Family Care Centres, University of Western Sydney, Civil Chaplaincies Advisory Committee, Department of Housing, the RTA and Centrelink
- “Memorandum of Understanding Register” policy
- “Operations Procedures Manual” particularly sections 8.25 & 21
- “Personal files” policy and guidelines (this concerns the “P” file kept for each member of staff)
- “Privacy internal review applications lodged out of time” policy
- “Privacy policy for Department of Corrective Services Internet website”
- “Public Access to Records, Documents, Personal Information and Health Information”

Most of the above policies are listed in the Department’s Summary of Affairs (Summary) which is available on the Department’s website [www.dcs.nsw.gov.au](http://www.dcs.nsw.gov.au) and are therefore available to the public. The Summary advises how the documents can be obtained.

## **12. Dissemination of policies and procedures to staff of the Department of Corrective Services**

The Plan is available on the Department's Internet and intranet sites. Staff have been made aware of the Plan. The majority of policies and documents at sections 10 and 11 are available to staff on the intranet.

Current policies will be reviewed to ensure that they adequately address the requirements of all the IPPs and HPPs.

A training module on the PPIP Act's and HRIP Act's requirements will be developed and incorporated into the curricula of the primary training courses for correctional officers and probation and parole officers, and in the Department's Common Induction Training.

Staff members who apply for computer access are required to declare that they have read, understood and agree to be bound by the Department's "Information Security Policy", "DCS Online Policy" and "IC&T Electronic Mail Policy". The Department's Information System displays a warning to staff regarding the appropriate management of information.

The Department's Code of Conduct, deals with the use and disclosure of information obtained in the course of employment. The Code of Conduct is also available on the Department's Internet and intranet sites.

Members of staff are kept up-to-date on privacy issues as they arise. Such information may be distributed by way of memoranda, instructions and articles in the "Corrective Services' Bulletin", which are all available on the intranet.

Staff can contact the Department's FOI & Privacy Unit for information and advice. Information about privacy and where to get further information is available on the intranet.

## 13. Consultants and Contractors

When the Department engages a consultant or contractor it uses the Consultancy Agreement (Agreement) that was developed by the Crown Solicitors' Office. Under the Agreement, consultants and contractors are to comply with relevant government policies. This includes, where relevant, legislation, policy, codes of practice or any other form of requirement concerning personal and health information. It is the Department's responsibility to draw the consultant's/contractor's attention to the relevant government policies. Where the consultant/contractor has access to personal and/or health information it is obliged under the Agreement to ensure that the information is protected against loss and against unauthorised access, use, modification or disclosure and against other misuse. Further details on the Agreement can be obtained from the Department of Premier and Cabinet's website, under 'publications', 'business and government', then 'consultancy agreement March 2005':

[http://www.dpc.nsw.gov.au/publications/publications/publication\\_list\\_-\\_new#1008](http://www.dpc.nsw.gov.au/publications/publications/publication_list_-_new#1008)

## 14. The Internal Review Process

- 14.1 An internal review is a process under Part 5 of the PPIP Act where agencies can handle complaints about how they have dealt with personal information and health information. Persons may also have privacy complaints handled by the Privacy Commissioner pursuant to part 4 of the PPIP Act or part 7 of the HRIP Act. Details should be sought direct from Privacy NSW.
- 14.2 Section 21 of the HRIP Act provides that the internal and external review processes under Part 5 of the PPIP Act are also applicable to complaints about the contravention of an HPP that applies to an agency and the contravention of a health privacy code of practice that applies to an agency.
- 14.3 Pursuant to section 52 of the PPIP Act and section 21(2) of the HRIP Act, an aggrieved person can apply to an agency for the review of conduct of that agency which he/she believes breaches:
- an IPP or an HPP
  - a privacy or health code of practice which applies to the agency
  - public register provisions
- 14.4 In the case of conduct relating to a contravention of an IPP, the relevant conduct must have occurred since 1 July 2000. In the case of conduct relating to a contravention of an HPP, the relevant conduct must have occurred since 1 September 2004.
- 14.5 Internal reviews conducted under Part 5 of the PPIP Act only apply to the conduct of a public sector agency and not to the actions of its employees who behave outside of their workplace duties and functions.
- 14.6 Pursuant to section 53(3) of the PPIP Act, applications for internal review must:
- (a) be in writing, and
  - (b) be addressed to the public sector agency concerned, and
  - (c) specify an address in Australia to which a notice under subsection (8) may be sent, and
  - (d) be lodged at an office of the public sector agency within 6 months (or such later date as the agency may allow) from the time the applicant first became aware of the conduct the subject of the application, and
  - (e) comply with such other requirements as may be prescribed by the regulations.
- 14.7 Application forms for an internal review under Part 5 the PPIP Act can be obtained from the Department's FOI & Privacy Unit. However, the use of a form is not necessary as long as the requirements of section 53(3) of the PPIP Act are met.
- 14.8 All people who complain about how the Department has dealt with their information should be advised in writing or verbally of their right to internal review under Part 5 of the PPIP Act. It is not necessary for a person to refer to an internal review to be advised of his or her right for an internal review. In addition, all people who unsuccessfully seek information or the amendment of information under the PPIP Act or the HRIP Act will be advised in writing of their right to internal review under the PPIP Act.
- 14.9 Complaints about personal or health information do not have to be dealt with through an

internal review. Where possible, people should be provided with alternative options for resolving their grievances. Importantly, where possible, information will be provided to an aggrieved person that may clarify the issue being complained about. For example, the conduct may be authorised by the Department's Code of Practice. The decision to go to an internal review is one that can only be made by the aggrieved person [as long as the application meets the requirements of section 53(3) of the PPIP Act]. The FOI & Privacy Unit will decide whether or not an application meets the requirements of section 53(3) of the PPIP Act.

14.10 An alternative to an internal review is writing to the Commissioner of the Department or a relevant senior officer of the Department and requesting that an issue be examined or addressed. In some circumstances the FOI & Privacy Unit may be able to resolve some issues. All inquiries should be directed to the Unit Manager on telephone: (02) 8346 1067.

14.11 All internal review applications to the Department, pursuant to Part 5 of the PPIP Act, will be co-ordinated by the FOI & Privacy Unit.

The FOI & Privacy Unit will ensure that the requirements of Part 5 of the PPIP Act are met, records of all internal review applications are maintained, and statistical details of any reviews are kept in order to meet the requirements of section 33(3)(b) of the PPIP Act. All internal review applications and outcomes will be recorded in a Register maintained by the FOI & Privacy Unit. All paperwork handled by the FOI & Privacy Unit for internal reviews will be held on a dedicated FOI & Privacy Unit file.

14.12 The FOI & Privacy Unit will fax to the Privacy Commissioner a notification of receipt of an internal review. Notification is by a set form that includes details of the applicant and a summary of the application. The application is not automatically faxed to the Privacy Commissioner. Full details of the application are provided in the Findings of the reviewer, which are faxed in full to the Privacy Commissioner along with a copy of this Department's final response to the applicant.

14.13 The FOI & Privacy Unit will send to the applicant a letter confirming receipt of the internal review application and will send to the applicant an "update letter" approximately four weeks after the commencement of the internal review. The same update letter will be faxed to the Privacy Commissioner.

14.14 The final response to an applicant includes a letter from the Commissioner of the Department, which contains the Commissioner's decision on the Findings of the internal review and a copy of the Findings. Pursuant to section 53(8), the Department attempts to notify applicants of the outcome of an internal review within 14 days after the completion of the review.

14.15 Departmental officers accused of wrongdoing in an internal review application will be notified in writing of that accusation and will be notified in writing of the Findings of the review and the Commissioner's decision in regard to the Findings of the review.

14.16 When the applicant is representing another person, the FOI & Privacy Unit will seek consent (verbally or in writing) for the applicant's name to be disclosed to an accused officer. The name of the person whose personal information is the subject of the application cannot be in all likelihood suppressed, because the officer would no doubt not be able to address the allegation without knowing the name of the person the subject of the complaint. Each case will be considered on an individual basis. If it is possible to suppress the name of the person whose personal information is the subject of the application, the Department will seek his or

her consent for the name to be released to the relevant officer. Consent does not have to be in writing.

- 14.17 In most cases an officer of the Department will conduct internal reviews. The person who conducts the review will be someone who was not substantially involved in any matter relating to the conduct the subject of the application. That officer will be asked to complete the internal review within 60 days from the day on which the application was received. An application will not be considered to have been “received” unless all the requirements of section 53(3) of the PPIP Act have been met; where necessary proof of identity or legal status has been provided; or where necessary the writer confirms that he/she would like an internal review to be undertaken.
- 14.18 Where necessary the officer undertaking the internal review will interview relevant persons, obtain and read relevant files and documents and refer to relevant legislation, policies and procedures. The reviewing officer may not necessarily contact the applicant.
- 14.19 The Commissioner of the Department considers the Findings of the internal review. The Commissioner may agree with the Findings in full, part or not at all. The decision to take any further action rests solely with the Commissioner. Once the Commissioner has made a decision on the review, the matter can be only examined again under the PPIP Act through the appeal process to the Administrative Decisions Tribunal or through any action that the Privacy Commissioner may decide to take. Internal reviews will not be “re-opened” through any other means. Clarification of the Findings in certain circumstances will be permissible.
- 14.20 Some possible findings of internal reviews are:
- alleged conduct occurred but the information concerned did not fall within the ambit of the PPIP Act or the HRIP Act;
  - the information subject to the alleged conduct did not fall within the ambit of the PPIP Act or the HRIP Act;
  - no evidence alleged conduct occurred;
  - insufficient evidence to suggest alleged conduct occurred;
  - alleged conduct occurred but complied with the IPPs / HPPs / public register provisions;
  - alleged conduct occurred; did not comply with the IPPs / HPPs / public register provisions; but non-compliance was authorised by an exemption, code or direction under section 41 of the PPIP Act or section 62 of the HRIP Act;
  - alleged conduct occurred; the conduct did not comply with the IPPs / HPPs / public register provisions; the non-compliance was not authorised (“a breach”);
  - alleged conduct did not occur, but an officer of the Department may be open to prosecution under section 62 or section 63 of the PPIP Act or section 68, 69 or 70 of the HRIP Act;

Following completion of the review the Department may:

- take no further action on the matter;
- make a formal apology to the applicant;
- take such remedial action as the Department thinks fit;
- provide an undertaking that the conduct will not occur again;
- implement administrative measures to ensure the conduct will not occur again;
- take other relevant action.