Health Care Complaints Commission

Privacy Management Plan

January 2013

Health Care Complaints Commission

Privacy Management Plan

Table of Contents

Health Care Complaints Commission - Management Plan

Privacy and Personal Information Protection Act 1998

1 Introduction

The Health Care Complaints Commission is required under the *Privacy and Personal Information Privacy Act 1998* (*PPIP Act*) to prepare a plan to indicate how it will comply with the requirements of this Act.

This plan includes:

- Policies and practices managing the Commission's compliance with the requirements of the PPIP Act
- How these policies and practices are communicated within the Commission
- Internal review arrangements
- Other matters and comments relevant to the Commission's management plan.

2 The role and functions of the Commission

The primary function of the Commission is to handle complaints about the professional practice and conduct of health practitioners and health services. This includes medical, nursing dental and other health services (such as chiropractors and psychologists) as well as health care practitioners who are not required to be registered such as masseurs and naturopaths.

Serious complaints may lead to disciplinary prosecutions of health practitioners before registration councils, professional standards committees, tribunals and courts. The Commission also has powers to make orders regulating unregistered health practitioners. The Commission also provides a resolution service that assists people to resolve complaints.

3 The legislative framework

3.1 Health Care Complaints Act 1993

Under section 99A of the *Health Care Complaints Act 1993*, it is an offence for any person to disclose information obtained in exercising the Commission's investigative functions unless the disclosure is made:

- With the consent of the person to whom the information relates, or
- In connection with the execution and administration of the *Health Care Complaints Act, or*
- For the purposes of any legal proceedings arising out of the *Health Care Complaints Act*, or any report of such proceedings, or
- With other lawful excuse
- Section 99B of the *Health Care Complaints Act 1993*, provides, however, that the Commission may disclose information to courts, police, authorities regulating health practitioners and others where the public interest in disclosing the information outweighs the public interest in protecting the privacy of any person to whom the information relates.

3.2 Privacy and Personal Information Protection Act 1998

The *PPIP Act* imposes obligations on public sector agencies in their handling of personal information. These obligations are set out in 12 Information Protection Principles ("IPPs") that govern the collection, use, disclosure, security and retention of personal information by agencies (see sections 8-19). The *PPIP Act* also provides individuals with a right of access to, and correction of, personal information held about them by agencies. The Commission is a public sector agency to which the *PPIP Act* applies. Under section 3, the Commission is an investigative agency and therefore subject to specified exemptions.

A copy of the IPPs (sections 8-19, *PPIP Act*) is at Appendix A.

Under the *PPIP Act*, there is provision for the making of a code of practice to modify the provisions of an IPP or its application to an agency. A code of practice may also be made to protect the privacy of individuals and for other purposes (see section 29, *PPIP Act*). The Privacy Commissioner is empowered under section 41 to issue directions to modify an IPP or exempt an agency from complying with an information protection principle or a privacy code of practice. There are presently two section 41 directions that are relevant to the Commission (these have been re-issued pending approval of codes of practice regarding the same matters) regarding:

- Information transfers between public sector agencies
- Processing of personal information by public sector agencies in relation to their investigative functions

Under the *PPIP Act* individuals are entitled to ask for an internal review of conduct they believe might breach the IPPs or a privacy code of practice. Further information about internal review is found below in part 6.

3.3 *Ombudsman Act 1974*

Pursuant to section 42 and 43 of the *Ombudsman Act*, the Commission is a signatory to a complaint referral arrangement and information sharing agreement with the Ombudsman, Anti-Discrimination Board, NSW Privacy and the Office of the Legal Services Commissioner. These arrangements authorise the referral of complaints and exchanges of information between agencies where appropriate.

3.4 *Health Records and Information Privacy Act 2002 (HRIPA)*

This Act applies to the Commission as an organisation that collects and holds private health information (section 11), with significant exemptions because the Commission is an investigative agency. Briefly, the Act allows health service providers to disclose private health information to the Commission if they reasonably believe the disclosure is necessary for the Commission to discharge its functions. Further, the Commission has the power under the *Health Care Complaints Act* to require the production of any information or documents. The HCCC is exempt from the use and disclosure of Health Privacy and Records when it is involved in complaint handling, otherwise HRIPA applies. The Health Information Protection principles at Schedule 1 of the HRIPA are set out in Appendix A.

3.5 *Privacy Act 1988 (Cth)*

Although this Act does not apply to the Commission's activities, it has relevance through its application to health providers and Commonwealth government authorities (such as the Health Insurance Commission) with whom we deal. The Federal Privacy Commissioner has also issued guidelines and other supporting information that deal specifically with health

related privacy.

4 Implications for the Commission of the Information Protection Principles

4.1 "Personal information"

Personal information is defined in section 4 as:

> information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.

Section 4(3) of the *PPIP Act* excludes various types of information from the definition of "personal information". For the Commission's purposes, these include:

- information about an individual who has been dead for more than 30 years
- information about an individual that is contained in a publicly available publication
- information about an individual arising out of a Royal Commission or Special Commission of Inquiry
- 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 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* (such as Cabinet documents or Executive Council documents)
- information or an opinion about an individual's suitability for appointment or employment as a public sector official.

Under the *PPIP Act*, personal information does not include unsolicited information (section 4(5)). It is the Commission's view that complaints made to the Commission are unsolicited – to determine otherwise would mean that under section 11 of the *PPIP Act*, the Commission is obliged to ensure this information is accurate, up to date, not excessive and complete. This is clearly outside the Commission's control.

Further, as an investigative agency, the Commission is specifically exempt from certain obligations under the *PPIP Act* that might impact upon its investigative and complaints handling activities.

The main categories of personal information held by the Commission are found at Appendix B.

4.2 Direct collection (section 9, *PPIP Act*)

The Commission is exempt from the obligation to collect information directly from an individual where:

- this might detrimentally affect (or prevent the proper exercise of) the Commission's complaint handling or investigative functions (section 24(1), *PPIP* Act) or
- non-compliance is lawfully authorised or required or permitted, necessarily implied or reasonably contemplated under any law (section 25, *PPIP Act*).

4.3 Limitations on use of personal information (section 17)

The Commission is exempt from complying with the requirement to use information only for the purpose for which it was collected if:

- it is reasonably necessary to enable the Commission to exercise its complaints handling or investigative functions (section 24(2) of the *PPIP Act*), or
- the use is lawfully authorised or otherwise permitted, necessarily implied or reasonably contemplated under any law (section 25 of the *PPIP Act*).

4.4 Limitations on disclosure of personal information (section 18)

The Commission may not disclose personal information to a person (other than the person to whom the information relates) or other body unless:

- The information is disclosed to the Independent Commission Against Corruption, Police Integrity Commission, NSW Ombudsman or Office of the Legal Services Commissioner (section 24(3) of the *PPIP Act*)..
- We are lawfully authorised or required to do so, or non-compliance is otherwise permitted, necessarily implied or reasonably contemplated under any law, for example, sections 12, 16, 17, 26 or s99B of the *Health Care Complaints Act*.
- The information is correspondence more properly dealt with by another public sector agency (see the Privacy Commissioner's direction pursuant to section 41 of the *PPIP Act* on "Information transfers between public sector agencies").
- The disclosure is reasonably necessary for the exercise of our investigative or complaints handling functions (see the Privacy Commissioner's direction pursuant to section 41 of the *PPIP Act* on "Processing of personal information by public sector agencies in relation to their investigative functions").

4.5 Special restrictions on disclosure of personal information (section 19)

The Commission is exempt from restrictions regarding disclosure of personal information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual activities (section 28(1), *PPIP Act*).

4.6 Corrupt disclosure and use of personal information by staff

Section 62 of the *PPIP Act* and Section 69 of the *HRIP Act* prohibits public sector officials from intentionally disclosing or using any personal information obtained through the exercise of his or her official functions. Allegation of this nature should be referred to the Police. The potential penalty for breach of this section is 100 units and/or imprisonment for 2 years. This prohibition does not prevent a public sector official from disclosing personal information about an individual if the disclosure is made in accordance with the *Protected Disclosures Act 1994* (section 62(3)).

4.7 Public registers

The Commission does not keep any public registers.

5 Compliance with the Information Privacy Principles

Privacy Principle (see Appendix A for the text of these)	Relevant legislative provisions, practices or policies
5.1 Complaint information	
Section 8: Collection of personal information is: ▪ for a lawful purpose ▪ reasonably necessary	▪ Practice manuals ▪ Privacy Management Plan and training ▪ Code of Conduct and Ethics ▪ Supervision of staff in the course of complaints handling, including investigations and file reviews
Section 9: Direct collection of personal information	▪ Exemption where compliance would impede the Commission's complaint handling or investigative functions under s24(1) ▪ Investigations might require collection from: - The holder of medical records such as a practitioner or health facility - Expert witnesses - Other government agencies holding relevant information such as the Department of Health, the Health Insurance Commission, Coroner's Office, the NSW Police Service or the Office of the Director of Public Prosecutions - Other persons or bodies relevant to the handling of the complaint or investigation
Section 10: Notification requirements: ▪ Name and contact details of agency ▪ That the information is being collected ▪ Use and disclosure ▪ Legal obligations to provide information ▪ Consequences of non-compliance ▪ Whether supply is voluntary ▪ Access/correction rights ▪ The purpose the information will be used for. ▪ The intended recipients of the information.	▪ Complaints exempt as unsolicited information (s 4(5), *PPIP Act*) ▪ Exemption where compliance would impede the Commission's complaint handling or investigative functions under s24(1), *PPIP Act* ▪ Notification included in: - Complaint form - Information requests to practitioners and health providers - Information requests to peer reviewers - Consent authority forms - General information brochures

Privacy Principle (see Appendix A for the text of these)	**Relevant legislative provisions, practices or policies**
Section 11: Information is: ▪ Relevant ▪ Accurate ▪ Not excessive ▪ Up to date ▪ Complete ▪ Not collected through unreasonable intrusion on an individual's private affairs	▪ Practice manual ▪ Privacy Management Plan and training ▪ Code of Conduct and Ethics ▪ Supervision of staff in the course of complaints handling, including investigations, prosecutions and file reviews
Section12: Retention and security of personal information	▪ Exemption regarding retention for longer than necessary: s 24(7) ▪ Appendix D to this Plan: Record keeping and security ▪ Records Management Plan and Records Disposal Schedule under *State Records Act* ▪ Code of Conduct and Ethics ▪ Privacy Guidelines and training
Section 13: Advice about personal information: ▪ Nature ▪ Purpose ▪ Access rights	▪ Exemption for information obtained during investigation process: s 25 – prohibition against disclosure unders99A, *Health Care Complaints Act* ▪ In all other cases, advice provided under the Commission's procedure on accessing personal information
Section 14: Right of access without excessive delay or expense	▪ Exemption for information relating to the Commission's complaints handling, investigative and reporting functions in relation to a complaint that is in the course of being dealt with (Schedule 2, *Freedom of Information Act* and s 25 *PPIP Act*) ▪ Exemption for information obtained during investigation process: s.25 – prohibition against disclosure unders99A, *Health Care Complaints Act* ▪ In all other cases, advice provided under the Commission's Personal Information Access and Correction Procedure
Section 15: Alteration of information	▪ Exemption for information relating to the Commission's complaints handling, investigative and reporting functions in relation to a complaint that is in the course of being dealt with (Schedule 2, *Freedom of Information Act* and s 25 *PPIP Act*) ▪ Exemption for information obtained during investigation process: s 25, *PPIP Act* ▪ In all other cases, advice provided under

Privacy Principle (see Appendix A for the text of these)	Relevant legislative provisions, practices or policies
	the Commission's procedure on access and correction of personal information
Section 16: Ensuring accuracy, relevancy, completeness prior to use	▪ Practice manuals ▪ Privacy Management Plan ▪ Code of Conduct and Ethics ▪ Supervision of staff in the course of complaints handling, including investigation and reviews ▪ Access to the registration databases of registration authorities
Section 17: Limits on use of information beyond purpose of collection	▪ s99A and s99B of *Health Care Complaints Act* regarding disclosure ▪ Investigations training materials ▪ Practice manual ▪ Privacy Guidelines and training ▪ Code of Conduct and Ethics ▪ Supervision of staff in the course of complaints handling, including investigations and reviews
Section 18: Limits on disclosure	▪ s99A and s99B of *Health Care Complaints* Act regarding disclosure ▪ S 26 of *Health Care Complaints Act* authority to disclose to other persons or bodies for investigation ▪ Disclosure to Office of Legal Services Commission, NSW Ombudsman, Privacy NSW, Anti-Discrimination Board pursuant to *Complaint Referral Agreement* under s 42-43 of *Ombudsman Act* ▪ Practice manuals ▪ Code of Conduct and Ethics ▪ Supervision of staff in the course of complaints handling, including investigations and reviews
Section 19: Special restrictions on disclosure of personal information	▪ Exemption under s 28(1) of the PPIP Act
Section 62: Prohibition on corrupt disclosure and use of personal information by public sector officials	▪ Code of Conduct and Ethics ▪ Prohibition under s99A of *Health Care Complaints Act* and good faith element

Privacy Principle (see Appendix A for the text of these)	Relevant legislative provisions, practices or policies
5.2 General administration files and file tracking systems	
Section 8: Collection of personal information is: ▪ for a lawful purpose ▪ reasonably necessary	General administration files and file tracking systems do not contain personal information
5.3 Employment records	
Section 8: Collection of personal information is: ▪ for a lawful purpose ▪ reasonably necessary	▪ Employment records are required to be kept under: - *Public Sector Employment and Management Act 2002* - *State Records Act 1998* - *Workers Compensation Act 1987* and other employment legislation - Government policies and awards
Section 9: Direct collection of personal information	▪ Commission practices in accordance with guidelines issued by the Premier's Department ▪ Pre-employment checks subject to consent
Section 10: Notification requirements: ▪ Name and contact details of agency ▪ That the information is being collected ▪ Use and disclosure ▪ Legal obligations to provide information ▪ Consequences of non-compliance ▪ Whether supply is voluntary ▪ Access/correction rights ▪ The purpose of collection ▪ The intended recipients of the information.	This is set out in job advertisements and /or information packages for applicants
Section 11: Information is: ▪ Relevant ▪ Accurate ▪ Not excessive ▪ Up to date ▪ Complete ▪ Not collected through unreasonable intrusion on an individual's private affairs	Employment and selection processes follow those set out in the *Public Sector Employment and Management Act 2002*, guidelines issued by the NSW Premier=s Department and other relevant employment legislation or awards

Privacy Principle (see Appendix A for the text of these)	**Relevant legislative provisions, practices or policies**
Section12: Retention and security of personal information	▪ The Commission is not required to comply with s 12(a) (retention for no longer than is reasonably necessary) pursuant to s 24(7), *PPIP Act* ▪ Employment information is kept for periods specified under the *State Records Act* and the Commission's Records Management Policy and Records Disposal Schedule ▪ Records are disposed of either by on-site shredding or placing in secure bins removed by security contractors ▪ Employment records are placed in locked cabinets or rooms when not in use with access limited ▪ Employment records are usually only forwarded to other public sector employers, who are subject to similar privacy regimes
Section 13: Advice about personal information: ▪ Nature ▪ Purpose ▪ Access rights	▪ Employees and job applicants provide the information to the Commission and are aware of what they provide. Information obtained from other sources is usually with the knowledge and consent of the person
Section 14: Right of access without excessive delay or expense	▪ Employees and former employees have supervised access to their records at negotiated times. This relates to personnel files only and does not pertain to recruitment files.
Section 15: Alteration of information	▪ As provided for under the *Public Sector Employment and Management Act 2002* and in accordance with government guidelines
Section 16: Ensuring accuracy, relevancy, completeness prior to use	▪ Obligation on employees to inform the Commission of any changes to personal information relevant to their employment
Section 17: Limits on use of information beyond purpose of collection.	▪ The Commission seeks consent before providing information protected by this section unless it is obliged by law enforcement or other legislation to release such information

Privacy Principle (see Appendix A for the text of these)	**Relevant legislative provisions, practices or policies**
Section 18: Limits on disclosure	▪ Employment information may be passed to other NSW public sector organisations when staff are transferred, promoted or re-appointed ▪ Personal information may also be disclosed to relevant authorities in relation to employment-related matters such as superannuation and health checks
Section 62: Prohibition on corrupt disclosure and use of personal information by public sector officials	▪ Code of Conduct and Ethics ▪ Prohibition under s99A and s99B of *Health Care Complaints Act*
Section 19: Special restrictions on disclosure of personal information	▪ The Commission is exempt from complying with s 19 pursuant to s 28(1), *PPIP Act* ▪ In any event, information of this type is provided voluntarily and with the consent of the person. Employment data (such as ethnicity) is provided in annual and other statistical reports in an aggregate way that does not identify particular individuals. In some circumstances health issues may be relevant to employment and these are handled as provided for under the *Public Sector Employment and Management Act 2002* and guidelines issued by the Premier's Department

6 Internal review procedure

6.1 Rights of internal review

Under Part 5 of the *PPIP* Act, and under the HRIP Act a person (the applicant) is entitled to ask the Commission to review allegations that the Commission has contravened an applicable IPP or privacy code of practice. The Commission will appoint an officer to conduct the review or deal with it personally.

Applications for review must be in writing.

6.2 The review process

The officer is responsible for managing the review process

will, upon receipt of a complaint:

- Acknowledge receipt of the complaint within 5 working days
- Notify the Privacy Commissioner as required by section 54 of the *PIPP Act*

The responsible officer will:

- Undertake the review, including:
    - Seeking further details from the applicant where necessary
    - Obtaining complaint/investigation files (if appropriate), policies and procedures
    - Interviewing relevant Commission staff
    - Identifying applicable privacy legislation, policies, guidelines and principles
    - Taking into account any information provided by the applicant and the Privacy Commissioner
- Determine the outcome of the review within statutory timeframes, documenting the investigation and reasons for the findings. Possible findings include:
    - No further action
    - Apology
    - Other remedial action (such as compensation)
    - Undertaking that the conduct will not occur again
    - Administrative measures to ensure the conduct will not occur again
    - Other appropriate action (such as correct incorrect personal information)
- Within 14 days of finalising the review:
    - Notification to the applicant, including the review's findings, any action to be taken (including reasons) and that the applicant is entitled to seek a review of those findings and proposed action by the Administrative Decisions Tribunal (section 53(8))
    - Advice to the Privacy Commissioner of the findings of the review and any proposed action to be taken (section 54(1)(c))

Complaints about privacy may also be made to the Privacy Commissioner. The Privacy Commissioner may deal with the complaint by:

- Referring it to the Commission for action or a response

- Conducting an investigation
- Seeking to resolve through conciliation

7 Compliance

7.1 Policies and procedures

The steps taken by the Commission to comply with its obligations under *the PPIP Act* include a review and amendment where appropriate of:

- this Management Plan
- documents used to collect/receive personal information such as the Commission's complaints form and letters seeking information from health service providers and other sources
- protocols between other agencies and organisations such as the Health Practitioner Councils, Health Conciliation Registry, Director of Public Prosecutions, Department of Health, Local Health Districts, Ombudsman and Legal Services Commissioner
- Commission policies such as its Code of Ethics and Conduct, email and internet policies
- the Commission's Records Management Procedures and Records Disposal Schedules
- the Commission's internal security arrangements

The Commission is also mindful of its obligations to comply with a range of government policies and procedures, including those issued by the Premier's Department and the Office of Information Technology.

7.2 Training and education

The Commissioner shall be responsible for the ongoing training and education of Commission staff (including any third party service providers or consultants) about their obligations under *the PPIP Act* by:

- ensuring the Privacy Management Plan remains up to date and available to all current and incoming staff through posting on the intranet and internet site
- informing staff of any changes to the plan through e-mail communication and staff meetings
- ensuring relevant privacy documents are consolidated and made available through the Commission's intranet
- conducting staff training sessions on privacy matters as required
- ensuring training materials are incorporated in the Commission's staff induction program
- providing ad hoc advice to staff

7.3 Contact Details

HCCC Privacy Officer

Ms Eiléan Hynes

HR Advisor and Executive Officer

02 9219 7455

ehynes@hccc.nsw.gov.au

Information and Privacy Commission NSW
email: ipcinfo@ipc.nsw.gov.au
phone: 1800 472 679.
office: Level 11, 1 Castlereagh Street, Sydney
office hours: 9am to 5pm Monday to Friday
http://www.ipc.nsw.gov.au/

Administrative Decisions Tribunal
phone: 9377 5711
Level 10, John Maddison Tower, 86-90 Goulburn Street, Sydney NSW 2000
Registry opening hours 9 am to 4.30 pm Monday to Friday except public holidays.
http://www.adt.lawlink.nsw.gov.au/

The HCCC Privacy Management Plan is available on line at
http://www.hccc.nsw.gov.au/Publications/Corporate-Documents

8 Reviewing and reporting on the Privacy Management Plan

The Commission is to review the plan whenever:

- the Commission wishes to introduce a new procedure for the collection, retention, use and disclosure of personal information; or
- a privacy code or a direction of the Privacy Commissioner, or the expiry of such a code or direction, modifies the application of the information protection principles to the Commission's operations

The Commissioner, on the advice of the Executive Officer, may amend this plan as necessary. A copy of the amended plan should be circulated to all Commission staff and the Privacy Commissioner as soon as possible after amendment.

8.1 Appendix A: The Privacy requirements under the Privacy and Personal Information Protection Act (PPIPA) and the Health Records Information Privacy Act (HRIPA)

PPIPA – Privacy Protection Principles

IPP 1: Section 8 – Collection of personal information for lawful purposes.

(1) A public sector agency must not collect personal information unless:

(a) The information is collected for a lawful purpose that is directly related to a function or activity of the agency, and
(b) The collection of the information is reasonably necessary for that purpose.

(2) A public sector agency must not collect personal information by any unlawful means.

IPP 2: Section 9 – Collection of personal information directly from individual

A public sector agency must, in collecting personal information, collect the information directly from the individual to whom the information relates unless:

(a) the individual has authorised collection of the information from someone else, or
(b) in the case of information relating to a person who is under the age of 16 years – the information has been provided by a parent or guardian of the person.

IPP 3: Section 10 – Requirements when collecting personal information

If a public sector agency collects personal information from an individual, the agency 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 of the following:

(a) The fact that the information is being collected
(b) The purposes for which the information is being collected
(c) The intended recipients of the information
(d) Whether the supply of the information by the individual is required by law or is voluntary, and any consequences for the individual if the information (or any part of it) is not provided
(e) The existence of any right of access to, and correction of, the information
(f) The name and address of the agency that is collecting the information and the agency that is to hold the information

IPP 4: Section 11 – Other requirements relating to collection of personal information

If a public sector agency collects personal information from an individual, the agency must take such steps as are reasonable in the circumstances (having regard to the purposes for which the information is collected) to ensure that:

(a) The information collected is relevant to that purpose, is not excessive, and is accurate up to date and complete, and
(b) The collection of the information does not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates

IPP 5: Section 12 – Retention and security of personal information

A public sector agency that holds personal information must ensure:

(a) That the information is kept for no longer than is necessary for the purposes for which the information may lawfully be used, and
(b) That the information is disposed of securely and in accordance with any requirements for the retention and disposal of personal information, and
(c) That the information is protected, by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse, and
(d) That, if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or disclosure of the information

IPP 6: Section 13 – Information about personal information held by agencies

A public sector agency that holds personal information must take such steps as are, in the circumstances, reasonable to enable any person to ascertain:

(a) Whether the agency holds personal information, and
(b) Whether the agency holds personal information relating to that person, and
(c) If the agency holds personal information relating to that person:
    (i) the nature of that information, and
    (ii) the main purposes for which the information is used, and
    (iii) that person's entitlement to gain access to the information.

IPP 7: Section 14 – Access to personal information held by agencies

A public sector agency that holds personal information must, at the request of the individual to whom the information relates and without excessive delay or expense, provide the individual with access to the information.

IPP 8: Section 15 – Alteration of personal information

A public sector agency that holds personal information must, at the request of the individual to whom the information relates, make appropriate amendments (whether by way of corrections, deletions or additions) to ensure that the personal information:

(a) is accurate, and
(b) having regard to the purpose for which the information was collected (or is to be used) and to any purpose that is directly related to that purpose, is relevant, up to date, complete and not misleading.

If a public sector agency is not prepared to amend personal information in accordance with a request by the individual to whom the information relates, the agency must, if so requested by the individual concerned, take such steps as are reasonable to attach to the information, in such a manner as is capable of being read with the information, any statement provided by that individual of the amendment sought.

If personal information is amended in accordance with this section, the individual to whom the information relates is entitled, if it is reasonably practicable, to have recipients of that information notified of the amendments made by the public sector agency.

IPP 9: Section 16 – Agency must check accuracy of personal information before use

A public sector agency that holds personal information must not use the information without taking such steps as are reasonable in the circumstances to ensure that, having regard to the purpose for which the information is proposed to be used, the information is relevant, accurate, up to date, complete and not misleading.

IPP 10: Section 17 – Limits on use of personal information

A public sector agency that holds personal information must not use the information for a purpose other than that for which it was collected unless:

(a) The individual to whom the information relates has consented to the use of the information for that other purpose, or
(b) The other purpose for which the information is used is directly related to the purpose for which the information was collected, or
(c) The use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual to whom the information relates or of another person.

IPP 11: Section 18 – Limits on disclosure of personal information

A public sector agency that holds personal information must not disclose the information to a person (other than the individual to whom the information relates) or other body, whether or not such other person or body is a public sector agency, unless:

(a) the disclosure is directly related to the purpose for which the information was collected, and the agency disclosing the information has no reason to believe that the individual concerned would object to the disclosure, or
(b) the individual concerned is reasonably likely to have been aware, or has been made aware in accordance with section 10, that information of that kind is usually disclosed to that other person or body, or
(c) the agency believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person.

If personal information is disclosed in accordance with subsection (1) to a person or body that is a public sector agency, that agency must not use or disclosure the information for a purpose other than the purpose for which the information was given to it.

IPP 12: Section 19 – Special restrictions on disclosure of personal information

A public sector agency must not disclose personal information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual activities unless the disclosure is necessary to prevent a serious or imminent threat to the life or health of the individual concerned or another person.

A public sector agency that holds personal information must not disclose the information to any person or body who is in a jurisdiction outside New South Wales unless:

(a) a relevant privacy law that applies to the personal information concerned is in force in that jurisdiction, or
(b) the disclosure is permitted under a privacy code of practice.

For the purposes of subjection (2), a relevant privacy law means a law that is determined by the Privacy Commissioner, by notice published in the Gazette, to be a privacy law for the jurisdiction concerned.

The Privacy Commissioner is, within the year following the commencement of this section, to prepare a code relating to the disclosure of personal information by public sector agencies to persons or bodies outside New South Wales.

Subsection (2) does not apply:

(a) until after the first anniversary of the commencement of this section, or
(b) until a code referred to in subsection (4) is made, whichever is the later.

HRIPA _ Health Information Protection Principles – Schedule 1

1 Purposes of collection of health information

(1) An organisation must not collect health information unless:
(a) the information is collected for a lawful purpose that is directly related to a function or activity of the organisation, and
(b) the collection of the information is reasonably necessary for that purpose.
(2) An organisation must not collect health information by any unlawful means.

2 Information must be relevant, not excessive, accurate and not intrusive

An organisation that collects health information from an individual must take such steps as are reasonable in the circumstances (having regard to the purposes for which the information is collected) to ensure that:
(a) the information collected is relevant to that purpose, is not excessive and is accurate, up to date and complete, and
(b) the collection of the information does not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates.

3 Collection to be from individual concerned

(1) An organisation must collect health information about an individual only from that individual, unless it is unreasonable or impracticable to do so.
(2) Health information is to be collected in accordance with any guidelines issued by the Privacy Commissioner for the purposes of this clause.

4 Individual to be made aware of certain matters

(1) An organisation that collects health information about an individual from the individual must, at or before the time that it collects the information (or if that is not practicable, as soon as practicable after that time), take steps that are reasonable in the circumstances to ensure that the individual is aware of the following:
(a) the identity of the organisation and how to contact it,
(b) the fact that the individual is able to request access to the information,
(c) the purposes for which the information is collected,

(d) the persons to whom (or the types of persons to whom) the organisation usually discloses information of that kind,
(e) any law that requires the particular information to be collected,
(f) the main consequences (if any) for the individual if all or part of the information is not provided.
(2) If an organisation collects health information about an individual from someone else, it must take any steps that are reasonable in the circumstances to ensure that the individual is generally aware of the matters listed in subclause (1) except to the extent that:
(a) making the individual aware of the matters would pose a serious threat to the life or health of any individual, or
(b) the collection is made in accordance with guidelines issued under subclause (3).
(3) The Privacy Commissioner may issue guidelines setting out circumstances in which an organisation is not required to comply with subclause (2).
(4) An organisation is not required to comply with a requirement of this clause if:
(a) the individual to whom the information relates has expressly consented to the organisation not complying with it, or
(b) the organisation is lawfully authorised or required not to comply with it, or
(c) 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
(d) compliance by the organisation would, in the circumstances, prejudice the interests of the individual to whom the information relates, or
(e) the information concerned is collected for law enforcement purposes, or
(f) the organisation is an investigative agency and compliance might detrimentally affect (or prevent the proper exercise of) its complaint handling functions or any of its investigative functions.
(5) If the organisation reasonably believes that the individual is incapable of understanding the general nature of the matters listed in subclause (1), the organisation must take steps that are reasonable in the circumstances to ensure that any authorised representative of the individual is aware of those matters.
(6) Subclause (4) (e) 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.
(7) The exemption provided by subclause (4) (f) extends to any public sector agency, or public sector official, who is investigating or otherwise handling a complaint or other matter that could be referred or made to an investigative agency, or that has been referred from or made by an investigative agency.

5 Retention and security

(1) An organisation that holds health information must ensure that:
(a) the information is kept for no longer than is necessary for the purposes for which the information may lawfully be used, and
(b) the information is disposed of securely and in accordance with any requirements for the retention and disposal of health information, and
(c) the information is protected, by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse, and
(d) if it is necessary for the information to be given to a person in connection with the provision of a service to the organisation, everything reasonably within the power of the organisation is done to prevent unauthorised use or disclosure of the information.
Note. Division 2 (Retention of health information) of Part 4 contains provisions applicable to private sector persons in connection with the matters dealt with in this clause.
(2) An organisation is not required to comply with a requirement of this clause if:
(a) the organisation is lawfully authorised or required not to comply with it, 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*).
(3) An investigative agency is not required to comply with subclause (1) (a).

6 Information about health information held by organisations

(1) An organisation that holds health information must take such steps as are, in the circumstances, reasonable to enable any individual to ascertain:
(a) whether the organisation holds health information, and

(b) whether the organisation holds health information relating to that individual, and
(c) if the organisation holds health information relating to that individual:
(i) the nature of that information, and
(ii) the main purposes for which the information is used, and
(iii) that person's entitlement to request access to the information.
(2) 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*).

7 Access to health information

(1) An organisation that holds health information must, at the request of the individual to whom the information relates and without excessive delay or expense, provide the individual with access to the information.
Note. Division 3 (Access to health information) of Part 4 contains provisions applicable to private sector persons in connection with the matters dealt with in this clause.

Access to health information held by public sector agencies may also be available under the *Government Information (Public Access) Act 2009* or the *State Records Act 1998*.

(2) 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*).

8 Amendment of health information

(1) An organisation that holds health information must, at the request of the individual to whom the information relates, make appropriate amendments (whether by way of corrections, deletions or additions) to ensure that the health information:
(a) is accurate, and
(b) having regard to the purpose for which the information was collected (or is to be used) and to any purpose that is directly related to that purpose, is relevant, up to date, complete and not misleading.
(2) If an organisation is not prepared to amend health information under subclause (1) in accordance with a request by the individual to whom the information relates, the organisation must, if so requested by the individual concerned, take such steps as are reasonable to attach to the information, in such a manner as is capable of being read with the information, any statement provided by that individual of the amendment sought.
(3) If health information is amended in accordance with this clause, the individual to whom the information relates is entitled, if it is reasonably practicable, to have recipients of that information notified of the amendments made by the organisation.
Note. Division 4 (Amendment of health information) of Part 4 contains provisions applicable to private sector persons in connection with the matters dealt with in this clause.

Amendment of health information held by public sector agencies may also be able to be sought under the *Privacy and Personal Information Protection Act 1998*.

(4) 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*).

9 Accuracy

An organisation that holds health information must not use the information without taking such steps as are reasonable in the circumstances to ensure that, having regard to the purpose for which the information is proposed to be used, the information is relevant, accurate, up to date, complete and not misleading.

10 Limits on use of health information

(1) An organisation that holds health information must not use the information for a purpose (a ***secondary purpose***) other than the purpose (the ***primary purpose***) for which it was collected unless:

(a) **Consent**
the individual to whom the information relates has consented to the use of the information for that secondary purpose, or

(b) **Direct relation**
the secondary purpose is directly related to the primary purpose and the individual would reasonably expect the organisation to use the information for the secondary purpose, or
Note. For example, if information is collected in order to provide a health service to the individual, the use of the information to provide a further health service to the individual is a secondary purpose directly related to the primary purpose.

(c) **Serious threat to health or welfare**
the use of the information for the secondary purpose 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) **Management of health services**
the use of the information for the secondary purpose is reasonably necessary for the funding, management, planning or evaluation of health services and:
(i) either:
(A) that purpose cannot be served by the use of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the use, or
(B) reasonable steps are taken to de-identify the information, and
(ii) if the information is in a form that could reasonably be expected to identify individuals, the information is not published in a generally available publication, and
(iii) the use of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

(e) **Training**
the use of the information for the secondary purpose is reasonably necessary for the training of employees of the organisation or persons working with the organisation and:
(i) either:
(A) that purpose cannot be served by the use of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the use, or
(B) reasonable steps are taken to de-identify the information, and
(ii) if the information could reasonably be expected to identify individuals, the information is not published in a generally available publication, and
(iii) the use of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

(f) **Research**
the use of the information for the secondary purpose is reasonably necessary for research, or the compilation or analysis of statistics, in the public interest and:
(i) either:
(A) that purpose cannot be served by the use of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the use, or
(B) reasonable steps are taken to de-identify the information, and
(ii) if the information could reasonably be expected to identify individuals, the information is not published in a generally available publication, and
(iii) the use of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

(g) **Find missing person**
the use of the information for the secondary purpose is by 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

(h) **Suspected unlawful activity, unsatisfactory professional conduct or breach of discipline**
the organisation:
(i) has reasonable grounds to suspect that:
(A) unlawful activity has been or may be engaged in, or
(B) a person has or may have engaged in conduct that may be unsatisfactory professional conduct or professional misconduct under the *Health Practitioner Regulation National Law (NSW)*, or
(C) an employee of the organisation has or may have engaged in conduct that may be grounds for disciplinary action, and
(ii) uses the health information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities, or

(i) **Law enforcement**
the use of the information for the secondary purpose 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

(j) **Investigative agencies**
the use of the information for the secondary purpose is reasonably necessary for the exercise of complaint handling functions or investigative functions by investigative agencies, or

(k) **Prescribed circumstances**
the use of the information for the secondary purpose is in the circumstances prescribed by the regulations for the purposes of this paragraph.

(2) 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*).

(3) The Ombudsman's Office, Health Care Complaints Commission, Anti-Discrimination Board and Community Services Commission are not required to comply with a provision of this clause in relation to their complaint handling functions and their investigative, review and reporting functions.

(4) Nothing in this clause prevents or restricts the disclosure of health information by a public sector agency:
(a) 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) to any public sector agency under the administration of the Premier, if the disclosure is for the purposes of informing the Premier about any matter.

(5) The exemption provided by subclause (1) (j) extends to any public sector agency, or public sector official, who is investigating or otherwise handling a complaint or other matter that could be referred or made to an investigative agency, or that has been referred from or made by an investigative agency.

11 Limits on disclosure of health information

(1) An organisation that holds health information must not disclose the information for a purpose (a ***secondary purpose***) other than the purpose (the ***primary purpose***) for which it was collected unless:

(a) **Consent**
the individual to whom the information relates has consented to the disclosure of the information for that secondary purpose, or

(b) **Direct relation**
the secondary purpose is directly related to the primary purpose and the individual would reasonably expect the organisation to disclose the information for the secondary purpose, or
Note. For example, if information is collected in order to provide a health service to the individual, the disclosure of the information to provide a further health service to the individual is a secondary purpose directly related to the primary purpose.

(c) **Serious threat to health or welfare**
the disclosure of the information for the secondary purpose 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) **Management of health services**
the disclosure of the information for the secondary purpose is reasonably necessary for the funding,

management, planning or evaluation of health services and:

(i) either:

(A) that purpose cannot be served by the disclosure of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the disclosure, or

(B) reasonable steps are taken to de-identify the information, and

(ii) if the information could reasonably be expected to identify individuals, the information is not published in a generally available publication, and

(iii) the disclosure of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

(e) **Training**

the disclosure of the information for the secondary purpose is reasonably necessary for the training of employees of the organisation or persons working with the organisation and:

(i) either:

(A) that purpose cannot be served by the disclosure of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the disclosure, or

(B) reasonable steps are taken to de-identify the information, and

(ii) if the information could reasonably be expected to identify the individual, the information is not made publicly available, and

(iii) the disclosure of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

(f) **Research**

the disclosure of the information for the secondary purpose is reasonably necessary for research, or the compilation or analysis of statistics, in the public interest and:

(i) either:

(A) that purpose cannot be served by the disclosure of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the disclosure, or

(B) reasonable steps are taken to de-identify the information, and

(ii) the disclosure will not be published in a form that identifies particular individuals or from which an individual's identity can reasonably be ascertained, and

(iii) the disclosure of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

(g) **Compassionate reasons**

the disclosure of the information for the secondary purpose is to provide the information to an immediate family member of the individual for compassionate reasons and:

(i) the disclosure is limited to the extent reasonable for those compassionate reasons, and

(ii) the individual is incapable of giving consent to the disclosure of the information, and

(iii) the disclosure is not contrary to any wish expressed by the individual (and not withdrawn) of which the organisation was aware or could make itself aware by taking reasonable steps, and

(iv) if the immediate family member is under the age of 18 years, the organisation reasonably believes that the family member has sufficient maturity in the circumstances to receive the information, or

(h) **Find missing person**

the disclosure of the information for the secondary purpose 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

(i) **Suspected unlawful activity, unsatisfactory professional conduct or breach of discipline**

the organisation:

(i) has reasonable grounds to suspect that:

(A) unlawful activity has been or may be engaged in, or

(B) a person has or may have engaged in conduct that may be unsatisfactory professional conduct or professional misconduct under the *Health Practitioner Regulation National Law (NSW)*, or

(C) an employee of the organisation has or may have engaged in conduct that may be grounds for disciplinary action, and

(ii) discloses the health information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities, or

(j) **Law enforcement**
the disclosure of the information for the secondary purpose 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) **Investigative agencies**
the disclosure of the information for the secondary purpose is reasonably necessary for the exercise of complaint handling functions or investigative functions by investigative agencies, or

(l) **Prescribed circumstances**
the disclosure of the information for the secondary purpose is in the circumstances prescribed by the regulations for the purposes of this paragraph.

(2) 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 organisation is an investigative agency disclosing information to another investigative agency.

(3) The Ombudsman's Office, Health Care Complaints Commission, Anti-Discrimination Board and Community Services Commission are not required to comply with a provision of this clause in relation to their complaint handling functions and their investigative, review and reporting functions.

(4) Nothing in this clause prevents or restricts the disclosure of health information by a public sector agency:
(a) 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) to any public sector agency under the administration of the Premier, if the disclosure is for the purposes of informing the Premier about any matter.

(5) If health information is disclosed in accordance with subclause (1), the person, body or organisation to whom it was disclosed must not use or disclose the information for a purpose other than the purpose for which the information was given to it.

(6) The exemptions provided by subclauses (1) (k) and (2) extend to any public sector agency, or public sector official, who is investigating or otherwise handling a complaint or other matter that could be referred or made to an investigative agency, or that has been referred from or made by an investigative agency.

12 Identifiers

(1) An organisation may only assign identifiers to individuals if the assignment of identifiers is reasonably necessary to enable the organisation to carry out any of its functions efficiently.

(2) Subject to subclause (4), a private sector person may only adopt as its own identifier of an individual an identifier of an individual that has been assigned by a public sector agency (or by an agent of, or contractor to, a public sector agency acting in its capacity as agent or contractor) if:
(a) the individual has consented to the adoption of the same identifier, or
(b) the use or disclosure of the identifier is required or authorised by or under law.

(3) Subject to subclause (4), a private sector person may only use or disclose an identifier assigned to an individual by a public sector agency (or by an agent of, or contractor to, a public sector agency acting in its capacity as agent or contractor) if:
(a) the use or disclosure is required for the purpose for which it was assigned or for a secondary purpose referred to in one or more paragraphs of HPP 10 (1) (c)–(k) or 11 (1) (c)–(l), or
(b) the individual has consented to the use or disclosure, or
(c) the disclosure is to the public sector agency that assigned the identifier to enable the public sector agency to identify the individual for its own purposes.

(4) If the use or disclosure of an identifier assigned to an individual by a public sector agency is necessary for a private sector person to fulfil its obligations to, or the requirements of, the public sector agency, a private sector person may either:
(a) adopt as its own identifier of an individual an identifier of the individual that has been assigned by the public sector agency, or
(b) use or disclose an identifier of the individual that has been assigned by the public sector agency.

13 Anonymity

Wherever it is lawful and practicable, individuals must be given the opportunity to not identify

themselves when entering into transactions with or receiving health services from an organisation.

14 Transborder data flows and data flow to Commonwealth agencies

An organisation must not transfer health information about an individual to any person or body who is in a jurisdiction outside New South Wales or to a Commonwealth agency unless:

(a) the organisation 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 for the implementation of pre-contractual measures taken in response to the individual's request, 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 organisation 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.

15 Linkage of health records

(1) An organisation must not:

(a) include health information about an individual in a health records linkage system unless the individual has expressly consented to the information being so included, or

(b) disclose an identifier of an individual to any person if the purpose of the disclosure is to include health information about the individual in a health records linkage system, unless the individual has expressly consented to the identifier being disclosed for that purpose.

(2) 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 the health information about the individual in the health records information system (including an inclusion for which an identifier of the individual is to be disclosed) 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).

(3) In this clause:

health record means an ongoing record of health care for an individual.

health records linkage system means a computerised system that is designed to link health records for an individual held by different organisations for the purpose of facilitating access to health records, and includes a system or class of systems prescribed by the regulations as being a health records linkage system, but does not include a system or class of systems prescribed by the regulations as not being a health records linkage system.

Appendix B: Categories of information held by the Commission.

The main categories of information held by the Commission are as follows:

Complaint information:

- Complaint files which may contain medical, financial, family, relationships and other information about the person lodging the complaint, the person on behalf of whom a complaint is lodged, the health care provider or health care organisation.

- A computerised complaint handling database and associated word processing documents which contain key or summary information about the complaint, witness statements or other information/evidence and investigation reports and related documents.

It should be noted that some of this information may be provided unsolicited to the commission (and is therefore excluded under *the PPIP Act*) and it therefore may or may not be relevant to the Commission's functions.

Employment records

- Employment records of Commission staff, former staff and job applicants.

Other records

- General administrative and policy documents and files which do not normally contain personal information.

Appendix C: Type of information held by the Commission

Complaints files and Databases

- Complainant details (name, address, telephone numbers)
- Patient details (sometimes not the person making the complaint)
- Health care provider details including areas of specialty
- Personal details of witnesses or others involved in the health care services or the complaint
- Information about particular characteristics or behaviour of the complainant, patient or health care provider
- Personal histories of people associated with the treatment or complaint including family and financial circumstances, relationships, business associations and, occasionally, criminal histories

Administrative

- Key/security card register
- Equipment on personal issue (long or short term) to staff
- Incident reports (includes workers= compensation incidents)
- Freedom of Information/privacy requests/files
- Payments made to individuals.
- Fringe Benefits Tax records
- Internal telephone lists
- Managers= after hours contact list.
- Use of motor vehicle and motor vehicle logs
- Records of cabcharge and like dockets issued

Employment

- Job applications
- Referee reports
- Employment contracts
- Medical examination reports
- Equal Employment Opportunity Information - gender, age ethnicity, disabilities
- Performance agreements (SPEADS)
- Work performance issues
- Identity documents - birth certificate, passport
- Staff addresses and contact information
- Copies of qualifications
- Bank account and payroll deduction details
- Payroll information
- Superannuation
- Tax File number and related exemption forms etc as applicable
- Group certificate information
- Probation forms
- Salary Increment forms
- Employment history including long leave records and transactions
- Injury and Workers compensation forms
- Leave forms
- Attendance records and associated summaries
- Confidentiality deeds
- Discipline matters

- Displaced officers
- Travelling subsistence and other allowances - may include dependent information etc
- Separation/termination information - exit questionnaire
- Workforce Profile Data information - Public Sector Management Office

Computers

- Commission documents, file and management records, accounting and payroll information.
- List of Access/logons.
- E-mail address books.
- Audit trails of access including Internet and E-mail.

Appendix D: Record keeping security

Item or Issue	Current or proposed practice or action
Complaints/Administration	
Administrative and Policy Files	- Maintained under the Commissioner's separate filing system.
Record Destruction	- Shredding on site, use of secure destruction bins/containers contractor or by the offsite records management contractor
Complaints Files	- Active files and exhibits etc to be protected from casual viewing by passing staff or visitors. This means even the name of the complainant or respondent on the file cover should not be visible as well as any documents (for example, place files face down in trays or on desks) - Files awaiting action to be kept in cabinets in offices or work stations - Inactive or closed files to be archived - Files in Records Room are in the custody of the Mail and Files Officer and may be accessed by staff authorised by Team or Section Managers. - File movements are electronically tracked in Casemate which is being integrated into the TRIM File Management System.
Incident reports	- If personal information is involved access as for Personal File
Payments/accounts payable	- Personal information not to be attached to vouchers. Cross reference to relevant file.
Fringe Benefits Tax records	- Access as for Personal File if related to salary packaging
Claims for loss or damage to personal effects	- If personal information is involved access as for Personal File
Staff Training and development records	- Usually will not contain confidential/personal information - If personal information is involved access as for Personal File

Item or Issue	Current or proposed practice or action
Employment	
Recruitment Files	- Placed in locked cabinet. - Access limited to Manager, Corporate Services, Manager, Human Resources, HR Advisor and Executive Support Officer and Commissioner - Running sheet to be placed on the top of the file indicating who accesses, why and when.
Personnel Files (Includes, employment contracts, proof of birth/identity, taxation forms, medical reports, leave applications, employment history, probation forms, salary increment forms if satisfactory, taxable travel/subsistence allowance EEO data Union membership.	- All Personnel Files are kept at ICAC - Electronically stored documents subject to password control hard copy records placed in locked cabinet when not being used by Staff Officer. - Access to paper files limited to relevant staff member.
Compensation Files	- As for Personal File
Performance Agreements	- Agreements are generally not confidential - Appraisal information to be placed in locked cabinet by relevant manager. - Access by Officer
Adverse work performance documents not contained elsewhere	- Placed in locked cabinet by relevant manager - Access by relevant staff member
Disciplinary records	- Placed in locked cabinet by relevant action officers while investigation and related action continues. - When action completed places in locked cabinet. - Access by Commissioner or nominee.
Workforce Profile Data	- Electronic copies to be subject to password access and documents identifying staff to be locked in cabinet. - Access by relevant officer.
Payroll data not on personnel files - including details of deduction payments to superannuation and health funds and unions etc.	- Reports or data containing personal information placed in locked cabinet. - Access by relevant Officer - -

Item or Issue	Current or proposed practice or action
Attendance/Flex Sheets	- Attendance records are not generally confidential but absences and the reasons may be. - Managers to keep secure from general staff viewing

Computers	
Stored data, including email	- Directories/data accessed via a password control system - Directory structure and access rights to reflect privacy and security. - Contractors to sign confidentiality agreements when issued with access rights. - System administrator log on and access rights approved by the Commissioner.
Backup of stored data	- Backup tapes or other media to be stored by a secure storage contractor or equivalent arrangement with another organisation.
Audit trails/access logs	- Applications with personal information to have audit trails /access logs - Audit / access reports to be stored in secure cabinet - Access to reports to be auhorised by the Commissioner or a Director
Databases	- Access provided as requested.