New South Wales

Personal Injury
Commission

Personal Injury Commission

Privacy Management Plan

Contents

Policy Statement

The New South Wales privacy laws do not affect the exercise of the Personal Injury Commission's judicial function in relation to hearing or determining proceedings before it. Documents, records and other material relating to proceedings are dealt with, as required, by the *Personal Injury Commission Act 2020* (PIC Act), enabling legislation and the *Personal Injury Commission Rules 2021* (PIC Rules). For example, decisions issued by the Commission are exempt from these privacy laws – see the Commission's Decision publication policy.

The Commission must comply with New South Wales privacy laws only in relation to the general management and administration of its Registry and office resources. The Privacy and Personal Information Protection Act 1998 (PPIP Act) and the Health Records and Information Privacy Act 2002 (HRIP Act) are the privacy laws in New South Wales. These laws set out privacy standards known as Information Protection Principles and Health Privacy Principles. These Acts and standards regulate the way we, collect, use, store and disclose personal and health information.

This Privacy Management Plan (PMP) meets the requirement for such a Plan under section 33 of the PPIP Act by demonstrating to members of the public how the Commission meets its privacy obligations under that Act and the HRIP Act and upholds and respects the privacy of our stakeholders, employees and others about whom we hold personal information.

The document is also for employees of the Commission, to explain how we comply with the requirements of the PPIP and HRIP Acts, and to prompt Commission employees, contractors and service providers to seek further advice where unsure about applicable privacy requirements. This PMP sets out the privacy obligations of the Commission, explains which exemptions the Commission commonly relies on and sets out the process for undertaking privacy internal reviews.

The scope of this PMP is explained in the introduction below. The Commission commits itself to operating in accordance with this PMP and regularly reviews its performance against this PMP. The Commission will review this PMP regularly and update it as required.

This document substantially adopts the Department of Customer Service (DCS) Privacy Management Plan. The Commission is an independent statutory Tribunal within the DCS cluster. The DCS Plan has been modified in-part to address the Commission's practices and procedures.

Definitions

Business Unit	A work unit performing a discrete business function within a government agency.
DCS	Department of Customer Service. The cluster of Government Agencies to which the Commission belongs.
Employee	Includes but is not limited to employees, members, consultants, contractors, agents and outsourced service providers performing work for the Commission.
Enabling Legislation	Enabling legislation is defined under section 5 of the *Personal Injury Commission Act 2020* (PIC Act) as: • workers compensation legislation, and • motor accidents legislation. Workers' compensation legislation includes: • *Workers Compensation Act 1987*, and • *Workplace Injury Management and Workers Compensation Act 1998*, and • any regulations, rules or instruments prescribed by these Acts. Motor accidents legislation includes: • *Motor Accidents Compensation Act 1999*, and • *Motor Accidents (Lifetime Care and Support) Act 2006,* and • Motor Accidents Injuries Act 2017, and • any regulations, rules or instruments prescribed by these Acts.

Health Privacy Principles (HPPs)	The 15 Health Privacy Principles are the key to the *Health Records and Information Privacy Act 2002*. These are legal obligations which NSW public sector agencies and private sector organisations must abide by when they collect, hold, use and disclose a person's health information. For further information see the Information and Privacy Commission factsheet "Health Privacy Principles".
Health Information	Defined in section 6 of the HRIP Act, health information is a type of 'personal information'. It includes but is not limited to: • information or an opinion about a person's physical or mental health, or a disability (at any time), such as a psychological report, blood test or x-ray; • personal information a person provides to a health service provider; • information or an opinion about a health service already provided to a person e.g., attendance at a medical appointment; • information or an opinion about a health service that is going to be provided to a person; • a health service a person has requested, and • some genetic information.
Health Information and Information Privacy Act 2002 (HIIP Act)	*Health Records and Information Privacy Act 2002*
Information Privacy Principles (IPPs)	The 12 Information Protection Principles are the key to the *Privacy and Personal Information Protection Act 1998*. These are legal obligations which NSW public sector agencies, statutory bodies, universities, and local councils must abide by when they collect, store, use or disclose personal information. For further information see the Information and Privacy Commission factsheet "Information Protection Principles".
People and Culture	The Human Resources arm of the DCS cluster of agencies.

Personal Information	Personal information is defined under section 4 of the *Privacy and Personal Information Protection Act 1998*. Personal information means 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.
Personal Injury Commission	The Personal Injury Commission as established under the *Personal Injury Commission Act 2020*.
Privacy and Personal Information Protection Act 1998 (PPIP Act)	*Privacy and Personal Information Protection Act 1998*
Privacy Officer	The Privacy Officer for the Commission is the Director, Legal and Policy. The Privacy Officer can be contacted by email at privacy@pi.nsw.gov.au or via the general inquiries number 1800 742 679.
Public Sector Agency	A 'public sector agency', as defined in section 3 of the *Privacy and Personal Information Protection Act 1998*. This includes a Public Service agency and a statutory body representing the Crown.
Sensitive Information	Means information referred to in section 19(1) of the *Privacy and Personal Information Protection Act 1998*. A special type of 'personal information' (see above). Some of the Commission's privacy obligations are different for 'sensitive information'. It means personal information that is also about a person's race, ethnicity, religion, sexuality, political or philosophical beliefs or membership of a trade union.

PART A: Introduction

Introduction to the Commission

The Commission resolves disputes between people injured in motor accidents and workplaces in NSW, insurers and employers.

The Commission is an independent statutory tribunal within the New South Wales justice system, committed to providing a transparent and independent dispute resolution service. The Commission was established under the *Personal Injury Commission Act 2020 (*PIC Act). The Commission exercises functions under the PIC Act and enabling legislation, regulations, rules and instruments.

The work of the Commission is undertaken by the President, Deputy Presidents, Division Heads, Principal Registrar, Members, Merit Reviewers, Mediators, and Medical Assessors, as well as legal and operational staff.

Information sharing and use within the Commission

The Commission is committed to the resolution of the real issues in dispute between parties in proceedings justly, quickly, cost effectively and with as little formality as possible.

The information collected for any Commission function may be used for a primary or directly related secondary purpose, as allowed under the PPIP Act. A primary purpose is the clear purpose for which we collect the information, for example information used to process an application for an assessment of permanent impairment. Directly related secondary purposes might include investigations, improvements in customer service, policy and programs, or responding to ministerial enquiries.

The Commission takes guidance from the Commission's Privacy Management Framework to ensure that the disclosure of information by one Commission division to another or to a public sector agency adheres to the information protection and health privacy principles.

Information sharing between Government Agencies

The Commission shares information public sector agencies including:

- State Insurance Regulatory Authority (SIRA);
- iCare;
- Medicare, and
- Australian Taxation Office.

The above list is not exhaustive. However, the Commission will only disclose personal information to other public sector agencies if the disclosure is directly related to the purpose for which the information was collected, and the Commission has no reason to believe that the individual concerned would object to the disclosure.

Disclosure is also permitted if the individual concerned is reasonably likely to have been aware, or has been made aware, that information of the kind that is disclosed, is of a kind that is usually disclosed to other public sector agencies.

Finally, disclosure of personal information may be made if the Commission 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.

Relevant Privacy Laws

The handling of personal and health information by the Commission is regulated by the following NSW privacy laws:

- *Privacy and Personal Information Protection Act 1998* (PPIP Act), and
- *Health Records and Information Privacy Act 2002* (HRIP Act).

The PPIP Act provides for the handling of "personal information" by public sector agencies. "Personal information" is any information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. The PPIP Act requires agencies to comply with 12 Information Protection Principles (IPPs).

The IPPs cover the full "life cycle" of information as it moves through an agency, from the point of collection through to the point of disposal. They include obligations with respect to data security, data quality (accuracy) and rights of access and amendment for the subject of personal information, as well as how personal information may be collected, used, and disclosed.

The HRIP Act provides for the handling of "health information" by public sector agencies. "Health information" is a special type of personal information. It includes information or an opinion about the physical or mental health or disability of an individual, a health service provided to an individual or other personal information collected to provide a health service.

The HRIP Act requires entities to comply with 15 Health Privacy Principles (HPPs). The HPPs are similar to the IPPs but are not identical. Like the IPPs, the HPPs cover the entire information "life cycle", but also include some additional principles with respect to anonymity, the use of unique identifiers, and the sharing of electronic health records.

There are exceptions and exemptions to many of the privacy principles and certain types of information are excluded from the definitions of “personal information” and “health information”, as set out in the PPIP Act, HRIP Act, related Regulations, Privacy Codes and Public Interest Directions.

Part 2, Division 3 of the PPIP Act provides for exemptions to the IPPs in certain situations.

For example, the Commission is not required to comply with:

- IPPs 2, 3, 6, 7, 8, 10, 11 or 12 if lawfully authorised or required not to comply, or compliance is otherwise permitted or is necessarily implied or reasonably contemplated under an Act or law, or
- IPP 2 (direct collection) if the information concerned is collected in relation to court or tribunal proceedings.

The Commission is not required to comply with IPPs with respect to collection, use or disclosure of personal information if the collection, use or disclosure of the information is reasonably necessary:

- to enable enquiries to be referred between the entities concerned, for example, for the use of corporate services of another agency. However, prior to doing so the agency will either deidentify all personal information before seeking advice from another agency or will obtain prior consent from the individual who the information is about before disclosure or may rely on any available exemptions; or
- to enable the auditing of the accounts or performance of a public sector agency or group of public sector agencies (or a program administered by an agency or group of entities), or
- to allow any of the entities concerned to deal with, or respond to, correspondence from a Minister or member of Parliament.

Public interest directions can modify the IPPs for any NSW public sector agency, and are available on the Information and Privacy Commission (IPC) website: https://www.ipc.nsw.gov.au/privacy/nsw-privacy-laws/health-public-interest-directions

Currently, there are no directions in operation that are likely to affect how the Commission manages personal information.

Our stakeholders

The Commission may collect personal or health information from, or disclose personal or health information, to stakeholders to undertake its work. These stakeholders include:

- parties to Commission proceedings;
- employees;
- regulators;
- law enforcement agencies;
- other, local, state, and federal government agencies and authorities;
- private sector companies;
- academics and researchers;
- medical and allied health professionals;
- non-government organisations;
- solicitors and other legal professionals;
- courts and tribunals, and
- Ministers and Parliament.

PART B: Responsibilities of all Commission employees

All employees of the Commission are required to comply with the privacy principles set out in the PPIP Act and HRIP Act. Both Acts contain criminal offence provisions applicable to employees who use or disclose personal information or health information other than in accordance with their lawful functions. Employees who are suspected of conduct that would breach the privacy principles or the criminal provisions may be disciplined for a breach of the Commission's Codes of Ethics and Conduct or the DCS Code of Ethics and Conduct. Suspected criminal conduct may result in dismissal of employment and/or referral to NSW Police. It is an offence to:

- intentionally disclose or use personal or health information accessed in doing our jobs for an unauthorised purpose;
- offer to supply personal or health information for an unauthorised purpose;
- attempt by threat, intimidation, etc, to dissuade a person from making or pursuing a request for health information, a complaint to the NSW Privacy Commissioner about health information, or an internal review under the HRIP Act, or
- hinder the Privacy Commissioner or member of staff from doing their job.

It is a criminal offence, punishable by up to two years' imprisonment, for any person to cause any unauthorised access to or modification of restricted data held in a computer. See s 62 of the PPIP Act, s 68 of the HRIP Act, and s 308H of the *Crimes Act 1900*.

Notification of a Data Breach

The Commission upon becoming aware of a data breach which involves personal or health information that may result in serious harm or having a reasonable suspicion that a data breach has occurred which is likely to result in serious harm, has a practice of voluntarily notifying the IPC and conducting an assessment to determine the circumstances of the breach or suspected breach, and of notifying stakeholders who may be at risk of suffering serious harm.

Privacy Officer for the Commission

Privacy officer

The Privacy Officer for the Personal Injury Commission is the Director, Legal and Policy.

The Privacy Officer can be contacted by email at privacy@pi.nsw.gov.au or via the general inquiries number 1800 742 679.

Responsibilities of the Privacy Officer

The Privacy Officer is responsible to:

- ensure the PMP remains up to date;
- publish the PMP;
- inform employees and stakeholders of any changes to the PMP;
- make a range of guidance material available to Commission employees, stakeholders and service providers to help them understand their privacy obligations, and how to manage personal and health information in their everyday work;
- provide privacy expertise to assist the adoption of a privacy-by-design approach to the development of new products and services, and to the existing products and services as they evolve;
- recommend controls to help manage privacy risks, and providing privacy expertise to assist their implementation;
- respond to privacy incidents;
- handle privacy complaints;

- maintain reporting on privacy incidents, complaints, and other relevant metrics;
- provide privacy training and awareness activities to Commission employees, stakeholders and service providers, and
- be available to answer any questions Commission employees may have about their privacy obligations.

In carrying out these responsibilities, the Privacy Officer may work with the privacy officers across the cluster, where appropriate.

The Privacy Officer is to ensure that the Commission's Annual Review includes:

- a statement of the actions taken in compliance with the requirements of the PPIP and HRIP Acts, and
- statistical details of any internal reviews conducted.

The Privacy Officer is to review and update this PMP:

- if the Commission wishes to introduce a significant new collection of personal information;
- if a privacy code or a direction of the Privacy Commissioner, or the expiry of such a code or direction, significantly modifies the application of the IPPs to the operations of the Commission, or
- at the conclusion of the calendar reporting year.

The Commission, on the advice of the Privacy Officer, may amend this Plan as necessary at any time. A revised copy of the Plan will be made available on the Commission website as soon as practicable. Any amendments will be drawn to the attention of all relevant personnel, and the NSW Privacy Commissioner will be advised of any such amendment as soon as practicable.

The Privacy Officer is also responsible for answering questions from members of the public about the content or operation of the PMP and handling any privacy complaints or non-routine requests for access to or correction of personal or health information.

PART C: Types of Personal and Health Information Held

There are two main categories of personal and health information that the Commission holds or has access to:

- personal and health information about members of the public and stakeholders relevant to the exercise of Commission functions ('Proceedings records'), and

- personal and health information about our employees, Members, decision-makers and service providers (‘employee and contractor records’).

Proceedings Records

To exercise our various functions and activities, we hold personal or health information such as:

- name, address and contact details;
- details of Motor Accident and Workers Compensation injuries, notifications, claims, and related decisions;
- medical reports, medical certificates and clinical notes from treating physicians;
- medical reports from independent medico-legal service providers;
- wage and other financial information;
- tax file numbers;
- payroll tax;
- employment details;
- job specifications and status;
- educational information;
- investigations;
- criminal records;
- records relating to births, deaths and marriages;
- signatures;
- complaints;
- interpreter use;
- Commission medical assessments, and
- details of claim settlements.

The above list is not exhaustive. The Commission may collect information electronically, via case management systems, email, over the phone and/or through audio-visual link platforms.

Employee Records

Staff of the Commission are employees of DCS. Employee records are generally held by DCS People & Culture on our behalf. However, the Commission also holds some information about its employees. The types of personal and health information the Commission holds about its employees includes:

- identity, demographic and contact data such as name, address, telephone numbers and email address, date of birth, gender, and signature;
- education records;
- payroll, attendance and leave records;
- bank account and financial records;
- performance management and evaluation records;
- referee reports;
- redundancy and termination decisions;
- workers' compensation records;
- work health and safety records;
- medical assessments, records, and certificates, and
- records of gender, ethnicity, and disability of employees for equal employment opportunity reporting purposes.

Employee Information

An employee of the Commission may access their own personnel file without cost. Apart from the employee the file relates to, others who may have authorised access to personnel files include People and Culture employees, nominated GovConnect employees and any other authorised delegates.

Where necessary, People and Culture may be required to arrange a health assessment for an employee. In doing so, People and Culture may be required to disclosure certain personal or health information to the organisation conducting the medical assessment who act as an agent for the Commission. Similarly, People and Culture may be required to disclose certain personal or health information to insurers in order to process an employee or claim.

Managers

To carry out their role, Commission employees in managerial roles may hold and have access to the personal information of employees who report to them. This information is held in SAP and may be held in Office 365 applications, including for example performance management and evaluation records.

Self-service function

Commission employees have access to some soft copy records contained in the DCS's enterprise business software used for managing employee information. This means employees have direct access to view and edit information, including applying for leave, viewing pay details, updating bank details, addresses, and email.

GovConnect

The Commission maintains most employee personnel files centrally. Case management of injured employees and investigations of workplace incidents are dealt with by the business unit known as People and Culture.

Day to day operations of most employees, such as leave requests and payroll, are administered by an outsourced company called GovConnect.

An Outsourcing Agreement was developed under the outsourcing program when GovConnect was engaged. It includes contractual arrangements providing that contractors must comply with the *Privacy Act 1988* (Cth), the PPIP and HRIP Acts, as well as any other privacy codes and policies in force, to ensure employees' personal information is protected. Certain employee details are disclosed to GovConnect for them to provide the payroll service.

The information held by People and Culture and GovConnect can include salary and payroll tax information, medical information, grievances and investigations, and employment history including disciplinary actions. Some information is maintained at a local division or business unit level, or is accessed by divisions or business units, for management purposes. This includes storing and using employees' personal and health information on internal databases for management purposes, case review and training. Human resource practices and procedures are governed by several pieces of legislation as well as various policies, procedures, and guidelines for the public service:

- *Government Sector Employment Act 2013* and associated Rules and Regulations;
- *Industrial Relations Act 1996* and associated Regulations;

- *Work Health and Safety Act 2011* and associated Regulations;
- *Workers Compensation Act 1987* and associated Regulations, and
- Any other relevant guidelines, policies or procedures from the NSW Ombudsman, the Public Service Commission, the Department of Premier and Cabinet, or other central oversight agencies.

The collection, use, storage, and disclosure of employee information is addressed in Part D below.

PART D: How the Commission manages personal and health information

This section explains how the Commission handles personal and health information. The PPIP Act and HRIP Act outline principles for managing personal and health information. These principles apply to all NSW government agencies and regulate the collection, storage, use and disclosure of personal and health information.

Addressing the principles

There are 12 IPPs set out in Part 2, Division 1 of the PPIP Act and 15 HPPs set out in Schedule 1 of the HRIP Act. The Information and Privacy Commission has issued fact sheets setting out the principles in summary.

Collection of personal information must only be for a lawful purpose (IPP 1 and HPP 1).

1.1 The principle in brief

We will only collect personal information and health information if:

- it is for a lawful purpose that is directly related to one of our functions, and
- it is reasonably necessary for us to have the information.

1.2 How the Commission applies this principle

The Commission will not collect personal information unless required for one of the Commission's functions. Some divisions and business units may also liaise with external stakeholders in order to fulfil Commission functions under legislation and the Commission will seek to access the personal and health information collected by those stakeholders if it is reasonably necessary for those functions.

The Commission may also use health information to lessen or prevent a serious threat to public health or safety, manage provision of health services, provide training, research purposes and for law enforcement purposes, including suspected unlawful activity and unsatisfactory professional conduct.

A substantial amount of personal and health information is collected from Commission employees for the purpose of personnel management. Such information is stored securely by the People and Culture unit and GovConnect, which have a centralised human resources management role. Personal and health information may also be collected directly from the employee within a division when it is lawfully authorised and necessary for employee management. For example, minimal health information may be collected by direct managers for the purpose of making necessary adjustments to allow employees to work, or for the creation of a return-to-work plan.

2. Personal information must only be collected directly from the person the information is about or someone authorised by that person (IPP 2 and HPP 3)

2.1. The principle in brief

The Commission collects personal information direct from the person unless that person has authorised otherwise. Health information is collected directly from the person unless it is unreasonable or impracticable to do so. The Commission will obtain some information from others where lawfully authorised to do this.

2.2. How the Commission applies this principle

The Commission collects personal and health information directly from the person unless the individual has authorised the Commission to do otherwise. However, there are circumstances when information may have been gathered from other sources, including other government agencies, an injured employee's doctor or parties to proceedings, where lawfully authorised to do this under a legislative provision or a Privacy Code of Practice.

Different parts of the Commission are required to gather certain personal information to carry out Commission functions. For example, personal and health information relating to workers compensation and motor accident compensation claims may be obtained from others, such as employers, insurers and scheme agents.

The Commission only obtains personal or health information from another source where it is lawfully authorised. Lawful authorisation may be provided by a specific legislative provision, consent, or through a legal instrument such as a Privacy Code of Practice. Provisions authorising collection from another source generally set out the limited circumstances in which the information can be gathered.

3. Notification when collecting personal information (IPP 3 and HPP 4)

3.1. The principle in brief

When collecting personal and health information from you, the Commission will take reasonable steps to tell you:

- who we are and how to contact us;
- what the information will be used for what other organisations (if any) we intend will receive this type of information from us;
- whether the collection is authorised by law or is voluntary;
- what the consequences will be if you do not provide the information to us;
- how you can access and correct your information held by us, and
- the name and address of the agency that is collecting the information and the agency that is to hold the information.

3.2. How the Commission applies this principle

When collecting health information about an individual from someone else, the Commission will take reasonable steps to that individual these things unless this would pose a serious health threat, or otherwise in accordance with NSW Privacy Commissioner guidelines.

The Commission endeavours to ensure all forms that collect personal or health information, such as application forms, etc, include clear privacy statements with the above information. The Commission will continue to review and refine the various forms across the Commission to ensure they meet this requirement.

Sometimes information may be collected by the Commission over the phone or face to face. Employees are trained to ensure they understand the privacy principles. Where appropriate, phone scripts will include a privacy statement to ensure employees provide information on the above points to you when they are collecting personal or health information from you.

4. How we collect personal information – the method and content (IPP 4 and HPP 2)

4.1. The principle in brief

When the Commission collects personal and health information from you, reasonable steps will be taken to ensure the information collected is:

- relevant, accurate, up-to-date, and complete, and

- not intrusive or excessive.

4.2. How the Commission applies this principle

The Commission will take reasonable steps to ensure that when we design forms, communicate with members of the public and employees (face to face, over the phone and in writing), or otherwise collect information from you, we do not seek personal or health information that is intrusive or excessive. The Commission will ensure that the personal and health information collected is relevant, accurate, up-to-date, and complete. The Commission will also make sure that, if you request it, you can see what information is held about you and the Commission will correct it as necessary.

Forms are designed to ensure that only information required to carry out Commission functions is requested or required from you. We will ensure these privacy principles are built into our contact centres' policies and practices through employee training and through phone scripts.

5. How we store and secure personal and health information (IPP 5 and HPP 5)

5.1. The principle in brief

The Commission takes reasonable security measures to protect personal and health information from loss, unauthorised access, modification, use or disclosure. The Commission is committed to ensuring personal and health information is stored securely, not kept longer than necessary, and disposed of appropriately.

5.2. How the Commission applies this principle

The Commission considers the security of information to be an important issue and has systems in place to ensure that only authorised people can access information. The PPIP Act provides several provisions for prosecuting individuals for unlawful disclosure of personal information, and s 308H of the *Crimes Act 1900* makes it an offence to access computerised records for a purpose other than official duties. Unlawful access to information by our employees, agents or contractors will result in disciplinary action, and in some serious cases, in criminal prosecution.

The Commission uses technical, physical, and administrative actions, as well as assessment by independent audit, as security measures to ensure personal and health information is stored securely. Some examples of retention and security measures that we have in place include:

- All our databases that are administered by the Commission's ICT area that hold personal or health information are restricted by password or other security measures to ensure that only people with a reason have access to that information. Some business units may have local databases using Microsoft Access or Excel that are only accessible to the employees who work in that area and therefore only relevant employees have access to the information;
- For Commission networks, a minimum password standard is applied, including that employees change passwords on a quarterly basis and be suitably complex;
- Multi-factor authentication as an additional security measure to validate identity when accessing online applications from outside of Commission networks;
- Secure destruction bins or paper shredders are provided for disposal of confidential paper records where necessary. System access warnings are given when access attempts to confidential systems are made;
- Security audits are conducted of electronic systems access and databases, and of access and exit from Commission premises, and
- Limiting access to sensitive information to only those who require access to perform lawful functions.

Access to electronic records keeping systems is restricted to the appropriate team, business unit or division, depending on the content, so that only those who need to access your data in order to carry out their functions can do so. Generally, once the data is entered into the secure system, any paper documents are shredded or sent for secure destruction to ensure that they cannot be accessed inappropriately.

Some areas maintain paper records, and these are stored either in a secure storage system onsite, such as lockable compactus or filing cabinet, or are sent to the Government Records Repository (GRR). GRR stores information in accordance with the provisions of the *State Records Act 1998* and standards issued by State Archives NSW.

6. Transparency (IPP 6 and HPP 6)

6.1. The principle in brief

Once the Commission has confirmed your identity, reasonable steps will be taken to let you find out:

- whether the Commission is likely to hold your personal or health information;
- the nature of the information the Commission holds;

- the purposes for which your personal or health information has been used by the Commission, and
- how you can access your information.

6.2. How the Commission applies this principle

The Commission has a broad obligation to the community to be open about how personal and health information is handled. This is different to collection notification which is specific and given at the time of collecting new personal or health information. Any information that is not required to be kept as a State record, and that is no longer needed to be kept, will be disposed of securely.

The PMP for the Commission will be available through the Commission website. It sets out the major categories of personal and health information that is held, explains the privacy obligations, and explains the process for accessing and/or amending any of the personal and health information the Commission holds about you.

7. Access to information we hold (IPP 7 and HPP 7)

7.1. The principle in brief

You can make enquiries at any time to find out if the Commission holds personal or health information about you. Once your identity has been confirmed, you may access your personal and health information without unreasonable delay or expense. The Commission will only refuse access where authorised by law. If requested, we will provide written reasons for any refusal in line with the Commission's commitment to be open and transparent.

7.2. How the Commission applies this principle

If you want a copy of your own personal or health information held by The Commission, it will usually be provided to you, free of charge, directly from the appropriate business unit. If you are having difficulties accessing your personal or health information, or you wish to make a formal application for information, you can contact the Commission's Privacy Officer.

8. Correction of information we hold (IPP 8 and HPP 8)

8.1. The principle in brief

Once your identity has been confirmed, you may update or amend your personal or health information held by the Commission to ensure it is accurate, relevant, up-to-date, complete, and not misleading.

8.2. How the Commission applies this principle

The Commission may wish to verify the accuracy of any information you request be amended, such as confirming the details of a motor accident claim with SIRA.

In general, any proposed corrections to your personal or health information should be provided in writing so the Commission can verify your identity and keep a record of the correction. You can send any requests for correction of your information to:

Director, Legal and Policy

Phone: 1800 742 679

Email: privacy@pi.nsw.gov.au

If the Commission does not agree to the correction or amendment, the reason for the refusal will be provided in writing to person the information refers to and the applicant requesting the amendment. The request to amend, and any reason for a refusal to amend, must be saved adjacent to the information it refers to for the life of the information record.

If the Commission corrects or amends a record, we will endeavour to contact any affected parties within 30 days of the change, and only where the notification is necessary to adhere to the principles outlined in this PMP. A disputed record may be a professional opinion that is challenged. However, the record of the professional opinion must be maintained regardless of the individual's request to vary that opinion.

9. Accuracy of information (IPP 9 and HPP 9)

9.1. The principle in brief

Before using personal or health information the Commission takes reasonable steps to ensure that the information is relevant, accurate, up-to-date, complete, and not misleading.

9.2. How the Commission applies this principle

The Commission ensures the accuracy of the information by collecting it directly from you wherever practicable, or otherwise in accordance with legislation. The Commission takes such steps as are reasonable in the circumstances to ensure that the information is relevant, accurate, up-to-date, complete, and not misleading. This may be achieved through the requirement of supporting documentation or by confirming the information with an outside agency.

Medical information will be verified in writing with the person to whom that information relates prior to that medical information being used or supplied to another party, such as a medical assessor. This gives you the opportunity to correct the information and allows the

Commission to ensure the information is relevant, accurate, up-to-date, complete, and not misleading prior to the use of the information. What might be considered 'reasonable steps' will depend upon all the circumstances, but some points to consider are:

- the context in which the information was obtained;
- the purpose for which we collected the information;
- the purpose for which we now want to use the information;
- the sensitivity of the information;
- the number of people who will have access to the information;
- the potential effects for you if the information is inaccurate or irrelevant;
- any opportunities we've already given you to correct inaccuracies, and
- the effort and cost in checking the information.

10. How we use personal and health information (IPP 10 and HPP 10)

10.1. The principle in brief

The Commission may use personal and health information:

- for the primary purpose for which it was collected;
- for a directly related secondary purpose;
- if we believe the use is necessary to prevent or lessen a serious and imminent threat to life or health;
- if it is lawfully authorised or required, or
- for another purpose, if you have consented.

10.2. How the Commission applies this principle

As a general principle, the Commission uses personal and health information collected only for the purpose for which it was collected. The relevant purpose should have been set out in a privacy notice at the time of collection.

The Commission may also use personal and health information for a directly related secondary purpose. A directly related secondary purpose is a purpose that is very closely related to the primary purpose for collection and would closely align with people's expectations around the use of their information. For example, the documents from an application for a medical assessment will be provided to a medical review panel or medical appeal panel where an application to refer the matter has been accepted.

There are several permitted purposes for using health information such as lessening or preventing a serious threat to public safety, managing health services, training, and research.

10.3 How the Commission uses personal and health information of employees

If you are a Commission employee, your personal and health information will be used for personnel management, such as salary payments, wellbeing in the workplace, and performance management. You have access to any of your own personal information that is held by the agency, for example through SAP, MyCareer and TRIM. This includes your payslips, leave balances, comments from your supervisor, timesheets, and other types of personal information. You are also entitled to access your personnel file or any other related human resources or employee safety and wellbeing files that contain your personal or health information.

Some information is maintained at a local divisional level or is accessed by divisions for management purposes. This includes storing and using employees' personal and health information on internal databases for management purposes (including employee resource planning), case review and training. You can request access to and amend your personal or health information at any time. This information will be updated without excessive delay.

11. How the Commission discloses personal and health information (IPP 11 and HPP 11)

11.1. The principle in brief

The Commission may disclose your information if:

- you have consented;
- the information is not 'health information' or 'sensitive information' and you have been made aware that the information is likely to be disclosed to the recipient;
- the information is not 'health information' or 'sensitive information', the disclosure is directly related to the purpose for which the information was collected, and we have no reason to believe you would object to the disclosure;
- if it is lawfully authorised or required;
- if it is reasonably necessary to lessen or prevent a serious threat to health, or
- the information is 'health information' and the disclosure is for the purpose for which the information was collected, or for a directly related secondary purpose within your reasonable expectations.

11.2. How the Commission applies this principle

The Commission may disclose information where lawfully authorised or required to disclose, such as where a public register is required to be kept by law.

Other disclosures the Commission makes will be appropriately related to the purpose for which the information was collected, or with your consent. The Commission may also disclose personal and health information to secondary service providers, such as consultants or investigators, where it is lawful and necessary for carrying out our functions. The Commission also discloses personal information to other government agencies where it is lawful.

For example, under section 13AA of the *Ombudsman Act 1974*, the NSW Ombudsman can request information from a public authority and the relevant provisions of the PPIP Act and HRIP Act do not apply to the agency's response to such a request.

When the Commission is required to disclose information to other public sector agencies, it will do so in accordance with the privacy laws.

12. Stricter rules apply to specific information (IPP 12 and HPP 14)

12.1. The principle in brief

Disclosing sensitive information (e.g., your ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities) is only allowed with your consent or if there is a serious and imminent threat to a person's life or health.

Disclosing personal or health information to someone outside of NSW, or to a Commonwealth agency, is only permitted in limited circumstances as set out in the legislation.

12.2. How we apply this principle

The Commission makes every effort to minimise the amount of information collected about your ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities. Where this information is collected, it is treated with the highest protection wherever possible.

The Commission only discloses personal or health information to someone outside NSW, or to a Commonwealth agency, if any of the following applies:

- they are subject to a law, scheme or contract that upholds principles substantially like the NSW IPPs or HPPs;
- you have consented;

- if it is necessary for a contract with you (or in your interests);
- if it will benefit you and it is impracticable to obtain your consent, but the Commission believes you would be likely to give your consent;
- the disclosure is reasonably believed by the relevant division or business unit to be necessary to lessen or prevent a serious and imminent threat to the life, health or safety of you or another person;
- the Commission has taken reasonable steps to ensure the information won't be dealt with inconsistently with the IPPs or HPPs. For example, where the Commission has bound the recipient by contract to privacy obligations equivalent to the principles, or
- if it is permitted or required by legislation or any other law.

13. How the Commission uses unique identifiers and linkage of health records (HPP 12, 13 and 15)

13.1. The principle in brief

The Commission may only assign identifiers (e.g., a number) to an individual's health information if it is reasonably necessary. The Commission must not include health information in a health records linkage system without your consent.

13.2. How the Commission applies this principle

People and Culture may collect health information to manage cases of injured Commission employees and to investigate workplace incidents. Where health information has been gathered to case manage an injured employee, it is not given a separate identifier but kept against the relevant employee's injury management record.

Where the information has been gathered as part of an investigation of a workplace incident, the information is held against the investigation file, and not given any separate identifier. People and Culture have no linkages to any health records systems.

When the principles do not apply

The IPPs and HPPs do not apply in certain situations or to certain information collected. Further details are provided in Appendix 2.

Some of the key situations where collection, use or disclosure of information is exempted from the compliance with certain IPPs and HPPs include:

- unsolicited information, unless the Commission has retained it for a purpose (although the Commission will generally treat unsolicited information in the same manner as information requested from you);
- personal information collected before 1 July 2000 (although the Commission will generally treat this information in the same manner as information collected after 1 July 2000);
- health information collected before 1 September 2004 (although the Commission will generally treat this information in the same manner as information collected after 1 September 2004);
- law enforcement and investigative purposes and some complaints handling purposes;
- when authorised or required by a subpoena, warrant or statutory notice to produce;
- if another law authorises or requires the Commission not to comply;
- where non-compliance is otherwise permitted, implied, or contemplated by another law;
- in the case of health information, to lessen or prevent a serious threat to public health or public safety;
- some research purposes;
- in the case of health information, compassionate reasons, in certain limited circumstances;
- finding a missing person, or
- information sent between public sector agencies to transfer enquiries or to manage correspondence from a Minister or member of Parliament.

Information published on public registers (Part 6 of the PPIP Act)

A public register is a register of information that is publicly available or open to public inspection. The Commission publishes a variety of decisions made by various decision-makers. The information published includes that which is required under s 58 of the PIC Act:

- decisions of the Commission;
- decisions of the President (or his delegate);
- decisions of merit reviewers under Division 7.4 of the *Motor Accident Injuries Act 2017*;

- decisions of review panels for merit reviewers under Division 7.4 of the *Motor Accident Injuries Act 2017*;
- decisions of Appeal Panels for medical assessments under Part 7 of Chapter 7 of the *Workplace Injury Management and Workers Compensation Act 1998*;
- decisions of review panels for medical assessments under Part 3.4 of the *Motor Accidents Compensation Act 1999* or Division 7.5 of the *Motor Accident Injuries Act 2017*, and
- any other decisions prescribed by the Rules.

If you do not wish to have your details published, you may request your information to be deidentified or redacted by making an application to:

(a) for proceedings being heard by the Commission that have not been completed—the Commission;

(b) for other proceedings that have not been completed—the President, or

(c) for proceedings that have been completed—the President within 7 days after the publishable decision is issued.

Any request for your information to be de-identified or redacted from a public register must be in writing, must provide reasons for the request, and should also include any evidence, such as a copy of a police report or apprehended violence order.

The Commission may use statistical information based on the personal information gathered in the exercise of our functions and employees for analysis, policy formulation, and process and service improvement. If this data is used outside of the business unit which collected it, we ensure it is de-identified so that no person can be recognised through the data.

PART E: Privacy and other legislation relating to personal and health information

Privacy legislation (NSW, Commonwealth and relevant international)

- *Privacy and Personal Information Protection Act 1998 (NSW)* (PPIP Act);
- *Privacy and Personal Information Protection Regulation 2019* (NSW);
- *Privacy (Tax File Number) Rule 2015 (Cth)* (TFN Rule);
- *Health Records & Information Privacy Act 2002 (NSW)* (HRIP Act);
- *Health Records and Information Privacy Regulation 2017* (NSW);

- Codes of Practice, Directions and Statutory Guidelines made under the PPIP and HRIP Act;
- *General Data Protection Regulation (EU)* (GDPR), and
- *Privacy Act 1988 (Cth)* (Privacy Act).

Other relevant legislation

- *Crimes Act 1900* (NSW);
- *Data Sharing (Government Sector) Act 2015 (NSW);*
- *Government Information (Information Commissioner) Act 2009 (NSW)* (GIIC Act);
- *Government Information (Public Access) Act 2009 (NSW)* (GIPA Act);
- *Government Information (Public Access) Regulation 2018;*
- Independent Commission Against Corruption Act 1988 *(NSW);*
- *Public Interest Disclosures Act 1994 (NSW)* (PID Act);
- *State Records Act 1998 (NSW);*
- *State Records Regulation 2015;*
- *Taxation Administration Act 1996 (NSW);*
- *Workplace Surveillance Act 2005 (NSW), and*
- Refer to Appendix 1 for further details.

PART F: Policies affecting processing of personal and health information

Policies affecting processing of personal and health information include:

- Commission codes of conduct and ethics;
- DSC Code of Ethics and Conduct;
- Privacy Management Framework, and
- other policy documents relating to records management and information security applied by the Commission.

PART G: How to access and amend personal information

In most cases, you have the right to access and amend the personal and health information the Commission holds about you, for example, if you need to update your contact details. The Commission must provide access to or amend personal or health information without excessive delay and without expense. The Commission does not charge any fees to access or to amend personal or health information unless you are lodging a formal application under the GIPA Act.

Formal and informal requests Informal requests

Informal Requests

An informal request simply means that you contact the relevant business unit within the Commission, or the Commission Privacy Officer, and ask for the information you are seeking. There are no fees required and no formal requirements to be met.

In many cases, the relevant business unit will be able to amend your personal or health information on the spot, but the Commission may require something in writing from you to safeguard the security and accuracy of the information being amended.

Formal Requests

Formal requests to access personal or health information can be made under the PPIP Act, HRIP Act or the GIPA Act, depending on the circumstances and the sensitivity of the information involved. The Commission will provide details on the form and specific details to be included in your application before it will be considered valid.

No fee is required if you are requesting information under the PPIP or HRIP Acts, however GIPA applications will require the application fee of $30 to be paid unless the fee is waived in accordance with provisions under the GIPA Act.

Formal requests for your personal or health information (whether you are a member of the public or an employee) should be sent to the Privacy Officer. The Office of the Privacy Commissioner, within the IPC, can also provide help and guidance about your rights to access your personal and health information.

Limits on accessing or amending other people's information

The Commission is usually restricted from giving you access to someone else's personal and health information. While the PPIP Act and the HRIP Act give you the right to access your own information, the Acts generally do not give you the right to access someone else's information. However, both the PPIP and HRIP Acts allow you to give the Commission

permission to collect your personal and health information from, and disclose it to, someone else. If you do require someone to act on your behalf, you will need to give the Commission your written consent.

The IPC's guide to Privacy and People with Decision-making Disabilities explains how to seek consent for a secondary use or disclosure of personal information from a person who has limited or no capacity.

If you are under 16, we can collect information directly from your parents or guardian. The PPIP and HRIP Acts enable the Commission to disclose your information to another person in limited circumstances, such as to prevent a serious and imminent threat to the life or health and safety of an individual. In the case of health information, other reasons include finding a missing person or for compassionate reasons in certain limited circumstances.

The GIPA Act may also allow your personal information to be provided to others if the public interest considerations in favour of disclosure outweigh the public interest considerations against disclosure. Each decision under the GIPA Act is made on a case-by-case basis and must take into whether personal information will be revealed, as well as any breach of the IPPs and HPPs, as public interest considerations against disclosure.

PART H: Privacy complaints

If you have any concerns about the way your personal or health information has been handled, or you disagree with the outcome of your request to access and/or amend your personal or health information, we encourage you first to discuss any concerns with the employee or business unit of the Commission dealing with your information (if known).

Any person may make a complaint:

- By making a general privacy complaint to the Commission;
- By applying to the Commission for an 'internal review' of the conduct they believe breaches an IPP and/or an HPP, which will lead to the Commission making findings and may result in some action being taken by the Commission, or
- Directly to the NSW Privacy Commissioner, which may lead to a conciliated outcome.

General privacy complaints

General privacy complaints may include stakeholders raising concerns (either in writing or verbally), to the Privacy Officer, for example, around the Commissions processes for handling their information, handling of a privacy breach or perceived miscommunication.

There are no external review rights to the NSW Civil and Administrative Tribunal (NCAT) at the conclusion of a general privacy complaint. If a person is not satisfied with the outcome of their 'general complaint' then they may still apply for a privacy internal review.

By law, a person has 6 months from first becoming aware of the relevant conduct to apply for an internal review. The Commission may decline to deal with an application for internal review received after that period.

The contact details for the Commission Privacy Officer are listed below.

Internal Review

General principles

If you have a complaint about the way your personal or health information has been handled or disagree with the outcome of your application to access and/or amend your personal and health information, we encourage you to discuss any concerns with the employee or division dealing with your information (if known).

You can also contact the Commission:

Director, Legal and Policy

Phone: 1800 742 679

Email: privacy@pi.nsw.gov.au

The following general principles are relevant to applications for internal review of privacy complaints:

- you may apply to the Commission for an 'internal review' of the conduct you believe breaches an IPP or HPP, or you may make a privacy complaint directly to the NSW Privacy Commissioner. For explanation of how we apply the IPPs and HPPs, check out 'Part D: How the Commission manages personal and health information';
- complaints to the Privacy Commissioner can only result in a conciliated outcome, rather than a binding determination;
- you cannot seek an internal review for an alleged/potential breach of someone else's privacy, unless you are an authorised representative of the other person, and
- an application for an internal review must be made within six months from when you first become aware of the conduct you are concerned about (in limited circumstances we may consider a late application for internal review).

See Part J for how to contact the IPC.

How to apply for internal review

Requests for internal review should be sent to privacy@pi.nsw.gov.au and needs to:

- be in writing;
- be addressed to the Commission;
- include a return address in Australia or a valid email address, and
- be lodged with the Commission within six months from the time the applicant first became aware of the conduct that they want reviewed, and their right to seek internal review.

Please complete the Commission's Privacy Complaint/Concern: Internal Review Application Form available on the PIC website. You may submit any other relevant material along with your application.

What you can expect from the Commission:

- your application will be acknowledged in writing and the acknowledgement will include an expected completion date.
- the internal review will be conducted by a Privacy Officer, or by another person who:
    - was not involved in the conduct, which is the subject matter of the complaint, and is an employee or an officer of the Commission, and
    - is qualified to deal with the subject matter of the complaint.
- The internal review (a review conducted internally within the Commission) will be completed within 60 days of receiving your application and we will inform you of the outcome of the review within 14 days. If the review is not completed within this time, you have the right to seek external review at NCAT. More information on external reviews is provided below.
- We will follow the Privacy Commissioner's Internal Review Checklist (available at ipc.nsw.gov.au) and consider any relevant material submitted by you and/or the Privacy Commissioner.
- A copy of the written complaint will be provided to the Privacy Commissioner.
- The Privacy Commissioner may make submissions to the Commission as part of the internal review process.
- In deciding, the Commission may:

- take appropriate remedial action;
- make a formal apology to you;
- implement administrative measures to prevent the conduct occurring again;
- undertake to you that the conduct will not occur again, and/or
- take no further action on the matter.

- You will be informed of the outcome as soon as practical following the completion of the review and within 14 days of the internal review being decided, including:
  - the findings of the review;
  - the reasons for those findings;
  - the action the Commission proposes to take;
  - the reasons for the proposed action (or no action), and
  - role of the NSW Privacy Commissioner

The PPIP Act requires that the Privacy Commissioner be informed of the receipt of an application for an internal review of conduct and receive regular progress reports of the investigation. In addition, the Commissioner is entitled to make submissions about the application for internal review.

When we receive your application, we will provide a copy to the Privacy Commissioner. We will then continue to keep the Privacy Commissioner informed of the progress of the internal review, the findings of the review and the proposed action to be taken by the Commission in response to the internal review. Any submissions made by the Privacy Commissioner to the Commission will be taken into consideration when making the decision.

See Part J for how to contact the IPC.

External Review

If you are unhappy with the outcome of the internal review, you can apply to NCAT to review the decision (an “external review”). Generally, you have 28 days from the date of our internal review decision to seek the external review. You may also apply to NCAT to conduct an external review if we have not completed your internal review within 60 days. NCAT may make orders requiring the Commission to:

- refrain from conduct or action which breaches an IPP, HPP or Code;
- perform in compliance with an IPP, HPP or Code;

- correct or provide access to information;
- provide an apology, or
- take steps to remedy loss or damage.

NCAT may also make an order requiring the Commission to pay damages if the applicant has suffered financial loss or psychological or physical harm because of the conduct.

PART I: Strategies for implementing and reviewing this plan

This plan is a commitment of service to our stakeholders of how we manage personal information and health information. As it is central to how we do business, we have made this plan easy to access and easy to understand for people from all kinds of backgrounds.

We aim to promote public awareness of this plan by publishing the plan on our website in a format that is accessible to the widest possible audience, regardless of technology or ability.

Commission Executive

Our Executive Team is committed to transparency about how the Commission complies with the PPIP Act and HRIP Act, which is reinforced by:

- endorsing the plan and making it publicly available;
- reporting on privacy in our annual review in line with relevant legislation, and
- using the plan as an everyday reference point for our privacy management practice.

Commission employees

The Commission makes sure its employees are aware of this plan and how it applies to the work they do by:

- training employees so they understand their privacy obligations and how they are to manage personal and health information;
- providing targeted training for those employees who work in areas with a higher exposure to the personal and/or health information of customers or employees, such as those who perform human resources functions, employees who process applications and claims, frontline counter and phone staff, and dispute resolution officers;
- providing refresher training so that employees maintain awareness of privacy in doing their daily business;

- writing this plan in a practical way so our employees can understand what their privacy obligations are, how to manage personal and health information in their work and what to do if unsure about their privacy obligations;
- publishing this plan together with any subordinate plans or Codes of Practice on the Commission's intranet, and
- highlighting the plan at least once a year (for example, during Privacy Awareness Week).

Reviewing this Plan

Our plan will be reviewed at a minimum every two years, but more frequently when legislative, administrative, or systemic changes occur that affect the way we manage the personal and health information we hold. If you have any feedback on this document, please contact the Commission Privacy Officer:

Director, Legal and Policy

Phone: 1800 742 679

Email: privacy@pi.nsw.gov.au

PART J - Contacts

The Information and Privacy Commission (IPC)

The NSW Privacy Commissioner's contact details are:

Phone: (02) 9619 8672

Email: ipcinfo@ipc.nsw.gov.au Web: www.ipc.nsw.gov.au

Mail: Information and Privacy Commission NSW GPO Box 7011 Sydney NSW 2001

Office: McKell Building, 2-24 Rawson Place, Haymarket NSW 2000

The NSW Civil and Administrative Tribunal (NCAT)

NCAT's contact details are:

Phone: 1300 006 228 and select the option Administrative and Equal Opportunity Division enquiries.

Email: aeod@ncat.nsw.gov.au

Web: www.ncat.nsw.gov.au

Mail: NSW Civil & Administrative Tribunal Administrative and Equal Opportunity Divisions PO Box K1026 Haymarket NSW 1240 | DX 11539 Sydney

Downtown Office: John Maddison Tower, 86-90 Goulburn Street, Sydney

Appendix 1:

Other related laws

This section contains a summary of other laws that may impact the way the Commission handles personal and health information.

Crimes Act 1900 (NSW) includes offences regarding accessing or interfering with data in computers or other electronic devices.

Data Sharing (Government Sector) Act 2015 (NSW) regarding the sharing of government data between government agencies and the government Data Analytics Centre, including the sharing of deidentified personal data. Enhanced privacy safeguards apply, and the usage of personal and health information must be in line with current privacy legislation.

Fair Trading Act 1987 (NSW) regarding the regulation of the supply, advertising and description of goods and services in NSW. Includes various provisions relating to the disclosure and sharing of information, for example, the publication of certain information for public access.

Government Information (Public Access) Act 2009 (NSW) (GIPA Act) and ***Government Information (Public Access) Regulation 2018*** under this law people can apply for access to government information we hold. Sometimes this information may include personal or health information. The Act contains public interest considerations against disclosure of information that would reveal an individual's personal information or contravene an information protection principle or health privacy principle under the PPIP and HRIP Acts.

If a person has applied for access to someone else's personal or health information we will usually consult with the affected third parties. If we decide to release a third party's personal information despite their objections, we must not disclose the information until the third party has had the opportunity to seek a review of the Commission's decision. When accessing government information of another NSW public sector agency in connection with a review, the Information Commissioner must not disclose this information if the agency claims that there is an overriding public interest against disclosure.

General Data Protection Regulation (EU) (GDPR) although a European privacy law, the GDPR is designed to have extra-territorial reach. The GDPR came into effect on 25 May 2018 and applies to any organisation offering goods or services to, or monitoring the behaviour of, individuals living in the European Union (EU). This could include some NSW public sector agencies, or vendors and suppliers to NSW public sector agencies.

Government Information (Information Commissioner) Act 2009 (NSW) (GIIC Act) under this law the Information Commissioner has the power to access government information held by other NSW public sector agencies for the purpose of conducting a review, investigation or dealing with a complaint under the GIPA Act and GIIC Act.

The Information Commissioner also has the right to enter and inspect any premises of an NSW public sector agency and inspect any record.

This Act also allows the Information Commissioner to provide information to the NSW Ombudsman, the Director of Public Prosecutions, the Independent Commission Against Corruption or the Police Integrity Commission.

For further information on the operation of the GIIC Act, contact the IPC (see Part J for how to contact the IPC).

Independent Commission Against Corruption Act 1988 ***(NSW)*** regarding the misuse of information.

Privacy Act 1988 **(Cth)** ***(Privacy Act)*** under the Privacy Act, the Australian Information Commissioner has several monitoring, advice, and assessment related functions regarding the handling of tax file numbers (TFNs).

The Privacy (Tax File Number) Rule 2015 ***(TFN Rule)*** issued under s 17 of the Privacy Act regulate the collection, storage, use, disclosure, security, and disposal of individuals' TFN information. The TFN Rule only applies to the TFN information of individuals and does not apply to TFN information about other legal entities such as corporations, partnerships, superannuation funds and trusts.

The TFN Rule is legally binding. A breach of the TFN Rule is an interference with privacy under the Privacy Act. Individuals who consider that their TFN information has been mishandled may make a complaint to the Office of the Australian Information Commissioner (OAIC).

Public Interest Disclosures Act 1994 ***(NSW)*** (PID Act) regarding disclosing information that might identify or tend to identify a person who has made a public interest disclosure.

State Records Act 1998 ***(NSW) and*** ***State Records Regulation 2015*** regarding the management and destruction of records.

Taxation Administration Act 1996 ***(NSW)*** regarding administration and enforcement of taxation laws. Division 3 of this Act includes secrecy provisions, including that a person who is or was a tax officer must not disclose any information obtained under or in relation to the administration of a taxation law, except as permitted under this Act.

Workplace Surveillance Act 2005 ***(NSW)*** regarding the regulation and legal use of camera, audio, computer surveillance and geographical tracking.

Appendix 2:

Exemptions

The PPIP and HRIP Acts contain exemptions from compliance with certain IPPs and HPPs. The main exemptions to each principle are:

Limiting the Commission's collection of personal and health information – IPP 1 and HPP 1

- unsolicited information
- personal information collected before 1 July 2000
- health information collected before 1 September 2004
- in the case of personal information, for certain Ministerial correspondence or referral of inquiries
- in the case of personal information, to enable the auditing of accounts of performance of an agency or agencies
- in the case of personal information, certain research purposes

How the Commission collects personal and health information – the source – IPP 2 and HPP 3

- unsolicited information
- personal information collected before 1 July 2000
- health information collected before 1 September 2004
- in the case of personal information, some law enforcement or some investigative and complaints handling purposes
- where another law authorises or requires the Commission not to comply with this principle
- where non-compliance is otherwise permitted, implied, or contemplated by another law
- in the case of personal information, where compliance would disadvantage the individual

Notification when collecting personal and health information – IPP 3 and HPP 4

- unsolicited information

- personal information collected before 1 July 2000
- health information collected before 1 September 2004
- the individual concerned has expressly consented to the non-compliance
- some law enforcement and investigative or complaints handling purposes
- where another law authorises or requires us not to comply
- where non-compliance is otherwise permitted, implied, or contemplated by another law
- where compliance would disadvantage the individual
- where notification about health information would be unreasonable or impracticable

How we collect personal and health information – the method and content – IPP 4 and HPP 2

- unsolicited information
- personal information collected before 1 July 2000
- health information collected before 1 September 2004
- law enforcement or some investigative and complaints handling purposes
- where another law authorises or requires us not to comply
- where non-compliance is otherwise permitted, implied, or contemplated by another law
- where compliance would disadvantage the individual

Retention and security – IPP 5 and HPP 5

- in the case of health information, the organisation is lawfully authorised or required not to comply
- in the case of health information, non-compliance is permitted under an Act or any other law

Transparency – IPP 6 and HPP 6

- if another law authorises or requires the Commission not to comply
- where non-compliance is otherwise permitted, implied, or contemplated by another law
- where the provisions of GIPA impose conditions or limitations (however expressed)

Access – IPP 7 and HPP 7

- some health information collected before 1 September 2004
- where another law authorises or requires the Commission not to comply
- where non-compliance is otherwise permitted, implied, or contemplated by another law
- the provisions of the GIPA Act that impose conditions or limitations (however expressed).

Correction – IPP 8 and HPP 8

- some health information collected before 1 September 2004
- some investigative or complaints handling purposes
- if another law authorises or requires the Commission not to comply
- where non-compliance is otherwise permitted, implied, or contemplated by another law
- the provisions of the GIPA Act that impose conditions or limitations (however expressed).

Accuracy – IPP 9 and HPP 9

- There are no direct exemptions to the operation of this principle.

Use – IPP 10 and HPP 10

- the individual concerned has consented to the non-compliance
- law enforcement and some investigative or complaints handling purposes where another law authorises or requires us not to comply
- where non-compliance is otherwise permitted, implied, or contemplated by another law
- in the case of health information, to lessen or prevent a serious threat to public health or public safety
- in the case of health information, finding a missing person
- information sent to other agencies under the administration of the same Minister or Premier for the purposes of informing the Minister or Premier
- some research purposes

- in the case of health information, some training purposes.

Disclosure – IPP 11 &12 and HPPs 11 & 14

- law enforcement and some investigative and complaints handling purposes
- when it is authorised or required by a subpoena, warrant or statutory notice to produce
- if another law authorises or requires the Commission not to comply
- where non-compliance is otherwise permitted, implied, or contemplated by another law
- in the case of health information, to lessen or prevent a serious threat to public health or public safety
- in the case of health information compassionate reasons in certain limited circumstances
- finding a missing person
- information sent to other agencies under the administration of the same Minister or Premier for the purposes of informing the Minister or Premier
- in the case of health information, some research and training purposes.

Identifiers – HPP 12

- There are no direct exemptions to the operation of this principle.

Linkage of health records – HPP 15

- health information collected before 1 September 2004
- where another law authorises or requires the Commission not to comply
- where non-compliance is otherwise permitted, implied, or contemplated by another law.

Appendix 3: Guide to drafting privacy collection notices

Where the Commission collects personal information from individuals, including for its own internal administrative purposes, it must make those individuals aware of the specified matters. The following principles guide the drafting of privacy notices within the Commission:

- the Privacy Officer must approve the wording and location of all privacy notices
- if the transaction can occur across more than one service channel/entity, the privacy notice should be worded as closely as possible across each channel/entity
- wording should be concise and in plain language
- the notice should clarify what the Commission will do with the information, as well as what any other entity or agency will do with the information
- the notice should be given / visible before any data collection begins
- notice can be provided on the paper forms developed by the entity or agency
- for digital transactions, the notice should be given on the landing page for that transaction, even if it also appears later in the process, and
- for digital transactions, if the data is being collected and stored by the Commission, the notice should also appear on the first data collection page.

At the end of each privacy notice it should be stated that for further information about privacy, contact the Privacy Officer.