NSW GOVERNMENT | Finance, Services & Innovation

Privacy Management Plan

Document Location

Ministerial Services - GIPA and Privacy team

Contents

INTRODUCTION

Our Department of Finance, Services and Innovation (DFSI) privacy management plan (PMP) explains how we manage personal and health information in line with NSW privacy laws.

Why we have a privacy management plan

We are required to have a PMP under the privacy laws. We are a large, diverse organisation and handle the personal and/or health information of many people across a range of areas. We take seriously our responsibility to look after the personal and health information of our customers and our staff and we are bound by law in the way we notify collection of, collect, use, store and disclose it. To help guide us in how we do this, section 33 of the *Privacy and Personal Information Protection Act 1998* (PPIP Act) requires that we have this PMP available.

In the DFSI PMP you will find information about:

- how to contact us with an enquiry or complaint about your personal or health information
- what to do if you think we have breached the PPIP Act or the *Health Records and Information Protection Act 2002* (HRIP Act)
- how to access and amend any personal and health information we hold about you.

Our PMP is intended to provide guidance on privacy management for the entire Department including each of our divisions. However, as DFSI includes a diverse range of divisions, each with multiple business units, some of them have individual PMPs to provide targeted business-specific guidance, tailored to the types of personal and health information they hold. The PMPs for DFSI divisions can be found at [DFSI privacy landing page to be created]. It is our intent that PMPs for individual DFSI divisions should be read in conjunction with this PMP as though they form part of it. Every effort has been made to draft this PMP and the divisional PMPs to be consistent, however, if any inconsistency arises, the PMP of the individual divisions take precedence.

Some divisions will also have a Privacy Code of Practice. This is a document approved by the NSW Privacy Commissioner that provides for specific exemptions from the Information Protection Principles in order to carry out their functions.

The following is a list of PMPs and Codes of Practice across DFSI:

- Service NSW Privacy Management Plan
- SIRA Privacy Management Plan
- SafeWork NSW Privacy Management Plan
- NSW Fair Trading Privacy Code of Practice

Internally, we use the DFSI PMP, in conjunction with any relevant divisional PMPs, to train our staff in handling personal and health information through mandatory training rolled out to all staff. We also use it for developing policies and procedures to ensure our compliance with privacy laws.

We've attempted to use plain English throughout the PMP to keep it user-friendly. If you're interested in further research on privacy, more information is available on the Information and Privacy Commission (IPC) website at www.ipc.nsw.gov.au

While we hope the DFSI PMP will answer many of your questions about privacy, please feel free to contact us either by email at privacy@finance.nsw.gov.au or by phone on our privacy information line: 02 9619 8672.

Definitions and abbreviations

The following terms are used in this PMP:

agency – this is a reference to a government department, either within NSW or another jurisdiction. DFSI is a government agency.

division – this is a reference to a broad business area within DFSI, often comprised of multiple business units. There are seven divisions in DFSI.

business unit – this is a reference to a work unit performing a discrete business function. Multiple business units make up divisions.

functions – as defined in section 3 of the PPIP Act, a function includes a power, authority or duty of a public sector agency.

personal information – as defined in section 4 of the PPIP Act, personal information is information or an opinion that identifies a person (or that would allow a person's identity to be discovered). Personal information can include:

- person's name, address, financial information and other details
- photographs, images, video or audio footage, and
- fingerprints, blood or DNA samples.

Some types of personal information are exempt from the definition of personal information eg. information about a person that has been dead for more than 30 years, information about someone that is contained in a publicly available publication or information or opinion about a person's suitability for employment as a public sector official.

health information – as defined in section 6 of the HRIP Act, health information is a specific 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 eg. 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

Sensitive information – used in this PMP to mean the information referred to in section 19(1) of the PPIP Act

DFSI – the Department of Finance, Services and Innovation.

SIRA – State Insurance Regulatory Authority

IPC – Information and Privacy Commission.

PMP – privacy management plan.

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

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

GIPA Act – the *Government Information (Public Access) Act 2009*.

PART 1 – ABOUT US

a. General

Who we are

DFSI is a service provider and regulator, operating through a number of divisions that deliver finance, service and innovation outcomes for the community and economy of NSW. This includes consumer protection, administration of State taxation and revenue collection, NSW land and property administration, sustainable government finances, major public works and maintenance programs, government procurement, information and communications technology and corporate and shared services.

We have seven divisions which carry out our functions:

Customer Transactions (comprising Service NSW and Titling and Registration Services) – deliver customer-facing transactions on behalf of all government agencies, providing a single point of contact for customers for a range of licensing and transactional services.

Regulation (comprising SafeWork NSW and NSW Fair Trading) – regulate, educate and provide services directly to individuals and businesses to create a fair, safe and equitable marketplace and investigate unfair practices. Provide regulatory services to ensure workplaces are safe. Regulate land titling systems in NSW.

SIRA – Regulate statutory insurance schemes to ensure insurance supports road users, workers and homeowners.

Property and Advisory – manage the leasing, utilisation, acquisition and disposal of significant property assets across government. Provide valuation, facilities management, place management and asset management advisory services across government.

Revenue (comprising the Office of State Revenue) – state revenue, taxation fines and debt collection programs.

ICT & Digital Government – drive whole of government reform in ICT, procurement and shared services and lead government's digital and data agenda.

Government Services – includes a range of specialised services such as whole-of-government procurement, spatial and surveying services, freedom of information and privacy services, and others.

We collect, hold, use and disclose personal and health information for the purpose of carrying out these functions and activities. A full breakdown of our structure and business units, as well as the DFSI Strategic Plan, is available on our website.

Our lead cluster minister is the Minister for Finance, Services and Property. Our other minister is the Minister for Innovation and Better Regulation.

Our stakeholders

We may collect personal or health information from, or disclose personal or health information to, our stakeholders to do our work. These stakeholders include:

- members of the public
- workers
- persons conducting a business or undertaking
- insurers
- other regulators
- other 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 representatives
- courts and tribunals
- Ministers and Parliament

Information sharing within DFSI

A strong focus of DFSI is on services and better regulation. The sharing of information between divisions and with other agencies can be vital to this goal. We take privacy seriously and manage your personal and health information with this goal in mind.

We collect and hold personal or health information that allows us to carry out our daily operations. This may include information required to process licence and certificate applications, workers compensation claims and disputes, consumer and trading complaints, land tax calculations or requests under right to information laws.

The information collected for any DFSI function may be disclosed (shared) across DFSI's divisions for a primary or directly related secondary purpose as allowed under legislation. A primary purpose is the clear purpose for which we collect the information from you, for example for a licence application. Directly related secondary purposes might include investigations, improvements in customer service, policy and programs, or responding to Ministerial enquiries.

We take guidance from the Privacy Governance Framework formulated by the Information and Privacy Commission (IPC) to ensure that the disclosure of information by one DFSI division to another adheres to the information protection and health privacy principles.

Your personal and health information is always handled in accordance with the privacy laws and principles.

Further information on how DFSI may disclose information across its divisions is outlined in point 11 of Part 2 of this plan.

Ministerial Services, GIPA and Privacy team

DFSI's Ministerial Services has a dedicated GIPA and Privacy team. In terms of its privacy functions, this team is responsible for:

- co-ordinating and, where appropriate, investigating privacy breaches and complaints
- establishing and maintaining a department wide Privacy Compliance Committee for compliance with and review of privacy policies and procedures
- ensuring the DFSI PMP remains up-to-date
- making a copy of this plan available to all current and incoming staff and contractors
- informing staff and contractors of any changes to the plan
- ensuring relevant privacy documents are consolidated and made available through DFSI's website.

To meet our annual reporting obligations each year, our annual report includes a statement of the action/s taken to ensure we comply with the requirements of the PPIP Act. The statement also provides statistical details of any review conducted, or conducted on our behalf, under the PPIP Act. DFSI's annual reports can be found on our website.

See Part 6 for our GIPA and Privacy team contact details.

b. Responsibilities of all DFSI staff

All employees, agents and contractors of DFSI are required to comply with the PPIP Act and HRIP Act. Both Acts contain criminal offence provisions applicable to staff, agents and contractors who use or disclose personal information or health information without authority. 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.

WARNING

It is a criminal offence, punishable by up to two years' imprisonment, an $11,000 fine, or both, for any person employed or engaged by DFSI (including former employees and contractors) to intentionally use or disclose any personal information or health information about another person, to which the employee or contractor has or had access in the exercise of his or her official functions, except in connection with the lawful exercise of his or her official functions.

c. Types of personal and health information we hold

What is personal and health information?

Different parts of DFSI may hold your personal information and in some cases, your health information.

Personal information

When we use the term personal information we mean it according to the definition in the PPIP Act (see Definitions in the Introduction section).

Health information

When we use the term health information we mean it according to the definition in the HRIP Act (see Definitions in the Introduction section).

Types of information held

Due to our diverse nature, the type of personal and health information held is equally diverse.

There are two main categories of personal and health information that we hold or have access to:

- personal and health information about members of the public and stakeholders
- personal and health information about our staff (employees and contractors).

Personal and health information held about members of the public and stakeholders

To exercise our various functions and activities, we hold personal or health information obtained through a person's workers compensation claim, NSW tax system information, fair trading or home building dispute, land title information, licence and certificate applications and so on. The following personal and health information may be collected, depending on the specific needs of the agency:

- Name and contact details
- Wages/Income details
- Home address
- Insurance information
- Job specifications and status
- Medical certificates and injuries
- Criminal records
- Date of birth
- Correspondence
- Payroll tax
- Financial and bank accounts
- Insurance claims history
- Land tax
- Compliance history
- Signatures
- Complaints
- Interpreter use
- Employment details
- Investigations
- Land title information
- Bankruptcy information

The above list is not exhaustive and we may also hold other personal or health information provided for a range of specific functions of our divisions. We may collect information electronically, via email or over the phone.

Personal and health information held about employees

We maintain most employees' personnel files centrally. Case management of injured staff and investigations of workplace incidents are dealt with by the DFSI business unit known as People and Culture. Day to day operations of most staff, 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. The transfer of employee records to GovConnect is appropriate in order for them to provide the payroll service.

Some staff in SIRA and SafeWork NSW are currently administered via a system known as Chris Pay and the People and Culture unit. It is intended that these staff will also be transferred to GovConnect in 2018 for day to day operational management.

The information held by People and Culture, GovConnect and Chris Pay 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
- *Industrial Relations Act 1996* and associated Regulation
- *Work Health and Safety Act 2011* and associated Regulation
- *Workers Compensation Act 1987* and associated Regulations
- The Public Service Commission's *Personnel Handbook*
- Any other relevant guidelines, policies or procedures from the NSW Ombudsman, the Public Service Commission, the Department of Premier and Cabinet, etc.

The collection, use, storage and disclosure of staff information are addressed in Part 2 below.

PART 2 – HOW WE MANAGE PERSONAL AND HEALTH INFORMATION

This section explains how we handle 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 Information Protection Principles (IPPs) set out in Part 2, Division 1 of the PPIP Act and 15 Health Privacy Principles (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. These are attached at Appendix 1.

As noted above, some divisions within DFSI may also have their own privacy management plan which should be read in conjunction with this plan.

1. Collection of personal information must only be for a lawful purpose (IPP 1 [PPIP s8] and HPP 1)

1.1. The principle in brief

We will only collect personal 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 we apply this principle

We won't collect personal information unless we need it for one of our functions. Some of our divisions and business units may also liaise with external stakeholders in order to fulfil our functions under legislation and we will seek to access the personal and health information collected by those stakeholders if it is reasonably necessary for those functions. For example, we may obtain personal information from a training provider when verifying qualifications for processing licence or certificate applications, or may obtain health information from an insurer for processing a workers compensation claim. Similarly, some divisions within DFSI may obtain personal or health information from other divisions within the agency where it is necessary to carry out our functions or for directly related secondary purposes authorised by law. An example of a directly related secondary purpose could include an investigation of a real estate licensee, using information collected for the issue of the licence.

A substantial amount of personal and health information is collected from our staff 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 staff member within a division, when it is lawfully authorised and necessary for staff management. For example, minimal health information may be collected by your direct manager for the purpose of making necessary adjustment to allow you to work, or for 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 [PPIP s9] and HPP 3)

2.1. The principle in brief

The various divisions within DFSI collect a range of information. We collect personal information direct from the person, unless they have authorised otherwise. We collect health information direct from the person, unless it is unreasonable or impracticable to do so. We will obtain some information from others (e.g. SIRA) where we are lawfully authorised to do this.

2.2 How we apply this principle

We collect your personal and health information directly from you, unless you have authorised us to do otherwise. However, there are circumstances when information may have been gathered from other sources, including other government agencies, where we are lawfully authorised to do this under a legislative provision or a Privacy Code of Practice.

Different parts of DFSI are required to gather certain personal information in order to carry out our functions. For example, health information relating to workers compensation and motor accident compensation fund

claims may be obtained from others, such as insurers and scheme agents. Likewise, complaints or disputes lodged with Fair Trading require one party to the dispute to provide the name and contact details of the opposing party so that Fair Trading can mediate or investigate the matter. Human resources personnel may need to liaise with an injured staff member's doctor. We will take what steps are necessary to ensure that collection of such information is done lawfully, such as getting consent from a staff member to contact their treating doctor.

We only obtain personal or health information from another source where it is lawfully authorised. Lawful authorisation may be provided by a specific legislative provision 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. For example, section 20 of the *Fair Trading Act 1987* allows a person appointed as an investigator under that Act to serve a notice on any person requiring the production of information, documents or evidence where it is relevant to a possible breach of that Act.

3. Notification when collecting personal information (IPP 3 [PPIP s10] and HPP 4)

3.1 The principle in brief

When collecting personal and health information from you, we 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) routinely receive this type of information from us
- whether the collection is authorised by law
- what the consequences will be if you do not provide the information to us, and
- how you can access and correct your information held by us.

3.2 How we apply this principle

When collecting health information about you from someone else, we take reasonable steps to tell you these things unless this would pose a serious health threat, or it is in accordance with NSW Privacy Commissioner Guidelines.[1]

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

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

4. How we collect personal information – the method and content (IPP 4 [PPIP s11] and HPP 2)

4.1 The principle in brief

When we collect personal and health information from you we will take reasonable steps to ensure the information we collect is:

- relevant, accurate, up-to-date and complete, and
- not intrusive or excessive

4.2 How we apply this principle

We will take reasonable steps to ensure that when we design forms, communicate with members of the public and staff (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. We will ensure that the personal and health information we do collect is relevant, accurate, up-to-date and complete. We may do this by checking the information directly with you, or by cross referencing the information with other sources, such as the Australian

[1] Statutory guidelines on the collection of health information from a third party are available from http://www.ipc.nsw.gov.au/resources-public-sector-agencies

Securities and Investment Commission's register of companies and business names, or with the Australian Tax Office's register of ABN numbers. We will also make sure that, if you request it, you have the opportunity to see what information we hold about you and we will correct it as necessary.

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

5. How we store and secure personal and health information (IPP 5 [PPIP s12] and HPP 5)

5.1 The principle in brief

We take reasonable security measures to protect personal and health information from loss, unauthorised access, modification, use or disclosure. We ensure personal and health information is stored securely, not kept longer than necessary, and disposed of appropriately.

5.2 How we apply this principle

We consider the security of information to be an important issue and have systems in place to ensure that only authorised people can access information. All employees, including contractors, are required to comply with the DFSI Code of Ethics and Conduct. In addition, the PPIP Act carries a number of provisions for prosecuting individuals for unlawful disclosure of personal information, and section 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.

We use 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 DFSI's ICT area that hold personal or health information are restricted by password or other security measures to ensure that only people with a lawful reason have access to that information. Some business units may have local databases using Microsoft Access or Excel. These databases are held on local drives that are only accessible to the staff who work in that area and therefore only relevant staff have access to the information.
- Network requirements are that staff change passwords on a quarterly basis.
- Secure recycling bins with locks are provided for disposal of confidential paper records where necessary, and shredders are provided where secure bins are not available.
- 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 DFSI premises.
- Limiting access to 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 a 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*.

In divisions that deal with substantial amounts of private or sensitive information, such as human resource units or investigation teams, access to the floor or room where personal or health information is stored may be restricted to authorised personnel.

6. Transparency (IPP 6 [PPIP s13] and HPP 6)

6.1 The Principle in Brief

Once we have confirmed your identity, we will take reasonable steps to let you find out:

- whether we are likely to hold your personal or health information

- the nature of the information we hold
- the purposes for which we used your personal or health information, and
- how you can access your information.

6.2 How we apply this principle

We have a broad obligation to the community to be open about how we handle personal and health information. This is different to collection notification (outlined in point 3 above), which is specific, and given at the time of collecting new personal or health information.

The PMP for DFSI and, where applicable, PMPs for individual divisions within DFSI, will be available through the DFSI website, any appropriate division's website and by request. These will set out the major categories of personal and health information that is held by the relevant division, explain the privacy obligations, and explain the process for accessing and/or amending any of the personal and health information we hold about you. The DFSI PMPs are listed on our [website] (– create a link when the landing page has been created).

7. Access to information we hold (IPP 7 [PPIP s14] and HPP 7)

7.1 The Principle in Brief

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

7.2 How we apply this principle

If you want a copy of your own personal or health information held by DFSI, we will usually be able to be provide it to you, free of charge, directly from the appropriate business unit. Sometimes your personal information may need a formal application under the GIPA Act, for example when your personal information contains the personal information of others.

Part 3 of this PMP sets out the process for accessing information held by DFSI divisions.

If you are having difficulties accessing your personal or health information, or you wish to make a formal application for information, you can contact our GIPA and Privacy team (see Part 6 for how to contact us).

8. Correction of information we hold (IPP 8 [PPIP s15] and HPP 8)

8.1 The Principle in Brief

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

8.2 How we apply this principle

DFSI divisions may wish to verify the accuracy of any information you request be amended, such as confirming qualifications with a training provider or information about a bankruptcy with the Bankruptcy Trustee.

In general, any proposed corrections to your personal or health information should be provided in writing so we can verify your identity and keep a record of the correction. You can send any requests for correction of your information directly to the appropriate business area or to our GIPA and Privacy team (see Part 6 for how to contact us).

9. Accuracy of information (IPP 9 [PPIP s16] and HPP 9)

9.1 The Principle in Brief

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

9.2 How we apply this principle

We ensure the accuracy of the information by collecting it directly from you wherever practicable, or otherwise in accordance with legislation (as set out in point 2 above).

We take 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. For example, an individual's previous involvement in a company may be verified through the Australian Securities and Investments Commission. A staff member's medical information will be verified in writing with the staff member 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 us 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 [PPIP s17] and HPP 10)

10.1 The Principle in Brief

We may use[2] personal and health information:

- for the primary purpose for which it was collected
- for a directly related secondary purpose (eg, Fair Trading might use information from a dispute you lodged in a wider investigation about the trader)
- 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 we apply this principle

As a general principle, we use the personal and health information we've 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.

We 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, information collected for a workers compensation claim may be accessed and used to investigate the complaint of an injured worker about the handling of their claim by a workers compensation scheme agent. Or information collected by Fair Trading to mediate a dispute may be accessed and used to investigate possible breaches of legislation.

There are a number of permitted purposes for using health information such as lessening or preventing a serious threat to public safety, managing health services, training, research, etc. The relevant exemptions for "use" of health information are summarised in more detail at Appendix 3.

How we use personal and health information of employees

If you are a DFSI 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 unlimited access to any of your own personal information that is held by the agency, for example through SAP, MyPerformance, or ChrisPay. This includes your payslips, leave balances, MyPerformance comments from your supervisor, timesheets and other types of personal information. You are also entitled to access your

[2] 'Use' is different to 'disclose'. We use information when we 'use' it internally.

personnel file, ATLAS 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, 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 we disclose personal and health information (IPP 11 [PPIP s18] and HPP 11)

11.1 The Principle in Brief

We may disclose[3] your information if:

- you have consented
- the information is not 'health information' or 'sensitive information' (see point 12 below for a definition of 'sensitive information' and how it is handled), 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 we apply this principle

We may disclose information we are lawfully authorised or required to disclose, such as where a public register is required to be kept by law. See point 14 below for more information about exemptions from the IPPs and HPPs and the type of information published on DFSI's public registers.

Other disclosures we make will be appropriately related to the purpose for which the information was collected and/or we will have your consent. We 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.

We also disclose 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 we are required to disclose information between DFSI divisions or with other public sector agencies, we will do so in accordance with the privacy laws.

12. Stricter rules apply to specific information (IPP 12 [PPIP s19] 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

We make every effort to minimise the amount of information we collect 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.

[3] 'Disclose' is different to 'use'. We disclose information when we provide it to someone outside the agency

We only disclose 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 similar to the NSW information protection principles or health privacy principles
- 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 we believe 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
- we have taken reasonable steps to ensure the information won't be dealt with inconsistently with the information protection principles or health privacy principles. For example, where we have bound the recipient by contract to privacy obligations equivalent to the principles
- if it is permitted or required by legislation or any other law, or
- if disclosure is exempted from the compliance with this principle for one of the reasons set out in point 14 below, for exmaple some research purposes.

We administer many laws that have equivalent laws in other states and territories. We will therefore liaise with agencies in other parts of Australia when it is lawful and necessary for carrying out our functions, such as verifying a person's licence status or compliance background in, or for, another state or territory.

13. How we use unique identifiers and linkage of health records (HPP 12, 13 and 15)

13.1 The Principle in Brief

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

13.2 How we apply this principle

Health information is generally only collected by our SIRA, SafeWork NSW and People and Culture business units. SIRA and SafeWork NSW have their own privacy management plans which provide more detail about how health information is stored and identified.

People and Culture may collect health information in order to manage cases of injured staff and to investigate workplace incidents. Where health information has been gathered to case manage an injured staff member, 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.

Other business units may inadvertently collect health information, even though it is not sought. For example, a person's medical condition may be disclosed to NSW Fair Trading during the mediation of a dispute in order to explain an absence from the mediation or the inability to complete an action in response to the dispute. When this sort of information is collected, it is not given any separate identifier and is not included in any health records linkage system.

14. Sometimes the Information Protection Principles and Health Privacy 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 3. 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 we have retained it for a purpose (although we will generally treat unsolicited information in the same manner as information we have requested from you)
- personal information collected before 1 July 2000 (although we will generally treat this information in the same manner as information collected after 1 July 2000)
- health information collected before 1 September 2004 (although we 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 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
- some research purposes
- in the case of health information, compassionate reasons, in certain limited circumstances
- finding a missing person, and
- information sent between public sector agencies to transfer enquiries or to manage correspondence from a Minister or member of Parliament.

* The privacy management plans of divisions within DFSI will provide examples of any relevant laws or circumstances that require or permit non-compliance with the IPPs or HPPs.

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. If you hold an authority that is required to be published on a public register such as a building licence, some of your personal information will be publicly available, such as your name, address, and any conditions placed on your licence.

Some of our public registers that may disclose personal information are:

- Conveyancers licence check
- Home building licence check
- Property services licence check
- Motor industry licence and certificate check
- Accommodation registers (retirement villages, boarding houses, residential parks)
- NSW Incorporated Associations Register
- Accredited building certifiers
- Torrens title register
- General register of deeds
- Water access licence register
- eTendering
- Asbestos assessor register

The above list is not comprehensive. If you are unsure whether information you have provided to DFSI may appear on a public register, please contact us and we can clarify this for you.

We only disclose personal information kept in the above registers in accordance with what is required or permitted under the relevant laws. If you have any specific concerns about your personal information being on a public register, you can contact the relevant business area within DFSI or our GIPA and Privacy team (see Part 6 for how to contact us). Any request for your information to be suppressed 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.

In making any decision to suppress your information, we will balance your rights with the public interest in maintaining public access to the information, in accordance with legal requirements.

Statistical information

We will use statistical information based on the personal information gathered from our customers and staff 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.

Sometimes we will publish statistical information on our websites. Whenever this is done, again the information is de-identified. For example, we publish data on the number of speeding fines issued by both the NSW Police or fixed speeding cameras. The number and value of the fines is aggregated, and no names or addresses are included, so that when another person is looking at the data, they cannot work out who it is referring to.

PART 3 – HOW TO ACCESS AND AMEND PERSONAL INFORMATION

In the majority of cases, you have the right to access and amend the personal and health information we hold about you, for example, if you need to update your contact details.

We must provide access to or amend personal or health information without excessive delay or expense. We do not charge any fees to access or amend personal or health information, unless you are lodging a formal application under the *Government Information (Public Access) Act 2009* (GIPA Act) (see below).

Formal and informal requests

Informal request

An informal request just means that you contact the relevant business unit within DFSI and ask for the information you are seeking. There are no fees required and no formal requirements to be met, such as a form, before your request will be actioned.

You can contact the relevant division or business unit within DFSI directly if you are trying to access or amend your information. You can also contact our GIPA and Privacy team (see Part 6 for how to contact us).

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

Formal request

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. You would generally need to complete a particular form and provide specific details before your application will be valid. An application under GIPA will usually be required if the personal or health information you want to access also contains information belonging to others, or would require a diversion of resources in order to comply with your request (such as a very large file that would take more than an hour to copy and collate for you). You can find out about making formal access applications under GIPA via our website.

No fee is required if you are requesting information under the PPIP or HRIP Acts, however GIPA applications will require the application fee to be paid.

Formal requests for your personal or health information (whether you are a member of the public or a staff member) should be sent to our GIPA and Privacy team (see Part 6 for how to contact us). Where there is a PMP for a particularly division or business unit within DFSI, this may also set out procedures for making formal access applications directly to the relevant area.

The Office of the Privacy Commissioner, within the Information and Privacy Commission (IPC), can also provide help and guidance about your rights around your personal and health information (see Part 6 for how to contact the IPC).

Limits on accessing or amending other people's information

We are 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 us 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 us your written consent. The IPC's guide to *Privacy and People with Decision-making Disabilities*[4] 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 are allowed to collect information directly from your parents or guardian.

[4] Available from www.ipc.nsw.gov.au

The PPIP and HRIP Acts enable us 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 account the fact that personal information will be revealed, as well as any breach of the IPPs and HPPs, as public interest considerations against disclosure.

PART 4 – YOUR REVIEW AND COMPLAINT RIGHTS

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 or amend your personal or health information, you have the right to both an internal review of the decision by DFSI or external review by the IPC or NCAT, depending on the situation.

Internal Review

General principles

We encourage you to contact us directly to resolve any concerns you have about our handling of your personal and health information.

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 staff member or division dealing with your information (if known). You can also contact us on the Privacy information line at 02 9619 8672 or by email at privacy@finance.nsw.gov.au.

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

- you may apply to DFSI 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 2: How we manage 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 6 for how to contact the IPC.

How to apply for internal review

To help you apply for an internal review, you can use the application form from the IPC. This can be downloaded from their website at www.ipc.nsw.gov.au. Although we encourage use of the form, it is not compulsory. You may submit any other relevant material along with your application.

Requests for internal review should be sent to DFSI's GIPA and Privacy team (see Part 6 for how to contact us) and needs to:

- be in writing
- be addressed to DFSI or the division within DFSI to which the complaint relates, and
- include a return address in Australia.

If the applicant is not literate in English and/or their first language and there is no organisation making the application on their behalf, the GIPA and Privacy team will use a professional interpreter where necessary.

What you can expect from us

- Your application will be acknowledged in writing and the acknowledgement will include an expected completion date.
- Either an officer in the GIPA and Privacy team (if they were not involved in the conduct which is the subject of the complaint), or another person not involved in the conduct which is the subject of the complaint, who is an employee or an officer of DFSI and is qualified to deal with the subject matter of the complaint, will conduct the review.
- The internal review will be completed within 60 days of receiving your application and we will inform you of the outcome of the review within 14 days of completing it. If the review is not completed within this time, you have the right to seek external review at the NSW Civil and Administrative Tribunal (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 give consideration to any relevant material submitted by you and/or the Privacy Commissioner.
- In making a decision, we may decide to:
    - take appropriate remedial action
    - make a formal apology to you
    - implement administrative measures to ensure that the conduct will not occur 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 within 14 days of the internal review being decided, including:
    - the findings of the review
    - the reasons for those findings
    - the action DFSI proposes to take
    - the reasons for the proposed action (or no action), and
    - your entitlement to have the findings and the reasons for the findings reviewed by NCAT.

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 us in response to the internal review. Any submissions made by the Privacy Commissioner to us will be taken into consideration when making our decision.

See Part 6 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"). You may also apply to NCAT to conduct an external review if we have not completed your internal review within 60 days. Generally you have 28 days from the date of our internal review decision to seek the external review.

NCAT has the power to make binding decisions on an external review, including ordering the payment of damages of up to $40,000.

For more information about seeking an external review, including current forms and fees, please contact NCAT (see Part 6 for how to contact NCAT)

PART 5 – CONTINUOUS IMPROVEMENT

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.

Promoting this Plan

Public awareness

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.

Additionally, we are required to make this plan publicly available as open access information under the *Government Information (Public Access) Act 2009*.

We aim to promote public awareness of this plan by:

- writing the plan in plain English
- publishing the plan on our website in a format that is accessible to the widest possible audience, regardless of technology or ability
- providing copies of the plan free of charge on request, and
- telling people about the plan when we answer questions about how we manage personal information and health information.

DFSI Executive

Our executive team is committed to transparency about how we comply 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 report in line with the *Annual Reports (Departments) Act 1985* and *Annual Reports (Departments) Regulation 2015*, and
- using the plan as part of induction for new employees, agents and contractors.

DFSI Employees

We make sure our staff are aware of this plan and how it applies to the work they do by:

- training staff so they understand their privacy obligations and how they are to manage personal and health information
- providing targeted training for those staff who work in areas with a higher exposure to the personal and/or health information of customers or staff, such as those who perform human resources functions, staff who process applications and claims, frontline counter and phone staff, and dispute resolution officers
- yearly refreshers so that staff maintain awareness of privacy in doing their daily business
- writing this plan in a practical way so our staff 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 our intranet, and
- highlighting the plan at least once a year (for example, during Privacy Awareness Week).

Part 6 - CONTACTS

DFSI's GIPA and Privacy team

For further information about this plan, the personal and health information we hold, or if you have any concerns, please feel free to contact the GIPA and Privacy team:

Phone: 02 9619 8672

Email: privacy@finance.nsw.gov.au

Web: www.finance.nsw.gov.au

Mail: Level 22, McKell Building, 2-24 Rawson Pl, Sydney NSW 2000

Visit: Documents, enquiries or complaints can be lodged via any Service NSW centre. The Service NSW centre locator can be found at https://www.service.nsw.gov.au/service-centre or by ringing Service NSW on 13 77 88.

The Information and Privacy Commission (IPC)

The NSW Privacy Commissioner's contact details are:

Phone: 1800 472 679

Email: ipcinfo@ipc.nsw.gov.au

Web: www.ipc.nsw.gov.au

Mail: PO Box R232 Royal Exchange NSW 2001

Office: Information & Privacy Commission, Level 3, 47 Bridge Street, Sydney NSW 2000

The NSW Civil and Administrative Tribunal (NCAT)

NCAT's contact details are:

Phone: 1300 006 228 and select Option 3 for all Administrative and Equal Opportunity Division enquiries

Web: www.ncat.nsw.gov.au

Post: NSW Civil & Administrative Tribunal, Administrative and Equal Opportunity Division, GPO Box 4005, Sydney NSW 2000.

PART 7 - APPENDICES

Appendix 1: Information Protection Principles and Health Privacy Principles

Appendix 2: Other related laws

Appendix 3: Exemptions

Appendix 1: Information Protection Principles and Health Privacy Principles

The Information Protection Principles (IPPs) explained for members of the public (IPC Fact sheet, September 2014)

The 12 Information Protection Principles (IPPs) are your key to the *Privacy and Personal Information Protection Act 1998* (PPIP Act)

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. As exemptions may apply in some instances, it is therefore suggested you contact the Privacy Contact Officer at the agency or the Information and Privacy Commission NSW (IPC) for further advice.

Collection

1. Lawful

An agency must only collect personal information for a lawful purpose. It must be directly related to the agency's function or activities and necessary for that purpose.

2. Direct

An agency must only collect personal information directly from you, unless you have authorised collection from someone else, or if you are under the age of 16 and the information has been provided by a parent or guardian.

3. Open

An agency must inform you that the information is being collected, why it is being collected, and who will be storing and using it. You must also be told how you can access and correct your personal information, if the information is required by law or is voluntary, and any consequences that may apply if you decide not to provide it.

4. Relevant

An agency must ensure that your personal information is relevant, accurate, complete, up-to-date and not excessive. The collection should not unreasonably intrude into your personal affairs.

Storage

5. Secure

An agency must store personal information securely, keep it no longer than necessary and dispose of it appropriately. It should also be protected from unauthorised access, use, modification or disclosure.

Access and accuracy

6. Transparent

An agency must provide you with details regarding the personal information they are storing, why they are storing it and what rights you have to access it.

7. Accessible

An agency must allow you to access your personal information without excessive delay or expense.

8. Correct

An agency must allow you to update, correct or amend your personal information where necessary.

Use

9. Accurate

An agency must ensure that your personal information is relevant, accurate, up to date and complete before using it.

10. Limited

An agency can only use your personal information for the purpose for which it was collected unless you have given consent, or the use is directly related to a purpose that you would expect, or to prevent or lessen a serious or imminent threat to any person's health or safety.

Disclosure

11. Restricted

An agency can only disclose your information in limited circumstances if you have consented or if you were told at the time they collected it that they would do so. An agency can also disclose your information if it is for a directly related purpose and it can be reasonably assumed that you would not object, if you have been made aware that information of that kind is usually disclosed, or if disclosure is necessary to prevent a serious and imminent threat to any person's health or safety.

12. Safeguarded

An agency cannot disclose your sensitive personal information without your consent, for example, information about ethnic or racial origin, political opinions, religious or philosophical beliefs, sexual activities or trade union membership. It can only disclose sensitive information without consent in order to deal with a serious and imminent threat to any person's health or safety.

The Health Privacy Principles (HPPs) explained for members of the public (IPC Fact Sheet, May 2014)

The 15 Health Privacy Principles (HPPs) are the key to the *Health Records and Information Privacy Act 2002* (HRIP Act).

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. Exemptions may apply, therefore it is suggested you contact the Privacy Contact Officer or the Health Information Manager in the organisation or agency in the first instance. Or contact the Information and Privacy Commission NSW (IPC) for further advice.

Collection

1. Lawful

An agency or organisation can only collect your health information for a lawful purpose. It must also be directly related to the agency or organisation's activities and necessary for that purpose.

2. Relevant

An agency or organisation must ensure that your health information is relevant, accurate, up-to-date and not excessive. The collection should not unreasonably intrude into your personal affairs.

3. Direct

An agency or organisation must collect your health information directly from you, unless it is unreasonable or impracticable to do so.

4. Open

An agency or organisation must inform you of why your health information is being collected, what will be done with it and who else might access it. You must also be told how you can access and correct your health information, and any consequences if you decide not to provide it.

Storage

5. Secure

An agency or organisation must store your personal information securely, keep it no longer than necessary and dispose of it appropriately. It should also be protected from unauthorised access, use or disclosure.

Access and accuracy

6. Transparent

An agency or organisation must provide you with details regarding the health information they are storing, why they are storing it and what rights you have to access it.

7. Accessible

An agency or organisation must allow you to access your health information without unreasonable delay or expense.

8. Correct

Allows a person to update, correct or amend their personal information where necessary.

9. Accurate

Ensures that the health information is relevant and accurate before being used.

Use

10. Limited

An agency or organisation can only use your health information for the purpose for which it was collected or a directly related purpose that you would expect (unless one of the exemptions in HPP 10 applies). Otherwise separate consent is required.

Disclosure

11. Limited

An agency or organisation can only disclose your health information for the purpose for which it was collected or a directly related purpose that you would expect (unless one of the exemptions in HPP 11 applies). Otherwise separate consent is required.

Identifiers and anonymity

12. Not identified

An agency or organisation can only give you an identification number if it is reasonably necessary to carry out their functions efficiently.

13. Anonymous

Give the person the option of receiving services from you anonymously, where this is lawful and practicable.

Transferrals and linkage

14. Controlled

Only transfer health information outside New South Wales in accordance with HPP 14.

15. Authorised

Only use health records linkage systems if the person has provided or expressed their consent.

Appendix 2: Other related laws

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

Government Information (Public Access) Act 2009 **(GIPA Act) and Government Information (Public Access) Regulation 2009**

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 our 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.

For more information on the operation of the GIPA Act and your personal information, please contact DFSI's GIPA and Privacy team (see Part 6 for how to contact us).

Government Information (Information Commissioner) Act 2009 **(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 a 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 6 for how to contact the IPC).

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

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

Independent Commission Against Corruption Act 1988 regarding the misuse of information.

Public Interest Disclosures Act 1994 **(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 and State Records Regulation 2015 regarding the management and destruction of records.

Appendix 3: Exemptions

The PPIP and HRIP Acts contain exemptions from compliance with certain IPPs and HPPs.

The main exemptions to each principle are:

Limiting our collection of personal and health information – IPP 1 [PPIP s8] 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 we collect personal and health information – the source – IPP 2 [PPIP s9] 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 us 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 [PIPP s10] 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 [PPIP s11] 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 [PPIP s12] 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 [PPIP s13] and HPP 6

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

Access – IPP 7 [PPIP s14] and HPP 7

- some health information collected before 1 September 2004
- where another law authorises or requires us 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 [PPIP s15] and HPP 8

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

Accuracy – IPP 9 [PPIP s16] and HPP 9

- there are no direct exemptions to the operation of this principle

Use – IPP 10 [PPIP s17] 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 [PPIP s18 and 19] 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 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 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 us not to comply
- where non-compliance is otherwise permitted, implied or contemplated by another law