Privacy Management Plan

March 2022

Policy Statement

This Privacy Management Plan (PMP) meets the requirement for such a Plan under section 33 of the *Privacy and Personal Information Protection Act 1998* (PIPP Act) by demonstrating to members of the public how Service NSW meets its privacy obligations under that Act and the *Health Records and Information Privacy Act 2002* (HRIP Act) and upholds and respects the privacy of our customers, employees and others about whom we hold personal information. It also acts as a reference for employees of Service NSW, to explain how we comply with the requirements of the PPIP and HRIP Acts, and to prompt Service NSW employees, contractors and service providers to seek further advice where unsure about applicable privacy requirements.

This PMP sets out the privacy obligations of Service NSW and its partner agencies, explains which exemptions Service NSW commonly relies on and sets out the process for undertaking internal reviews.

Service NSW commits itself to operating in accordance with this PMP and regularly reviewing its performance against this PMP. Service NSW will review this PMP quarterly at minimum, and update it as required.

This plan was last updated in March 2022.

Approved by			
Name:	Antonia Kendall		
Title:	Director, Privacy and Information Governance	**Date:**	16 March 2022

Privacy Management Plan

Contents

Definitions

Business Unit	A work unit performing a discrete business function within a government agency. Multiple business units make up divisions.
Health information	As 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 ▪ some genetic information.
Health Privacy Principles (HPPs)	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. The most up-to-date factsheet may be found at https://www.ipc.nsw.gov.au/health-privacy-principles-hpps-explained-members-public
Information Privacy Principles (IPPs)	The 12 Information Protection Principles (IPPs) are the 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. The most up-to-date factsheet may be found at

	https://www.ipc.nsw.gov.au/information-protection-principles-public
Partner agency	A NSW government agency, NSW Local Government, Commonwealth agency, other State or Territory government agency or non-government entity that Service NSW exercises functions for under delegation or by agreement.
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 using moderate steps, including by reference to other information). Personal information can include: a person's name, address, financial information, and other details including photographs, images, video, or audio footage. Some types of personal information are exempt from the definition of personal information e.g. 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.
Public sector agency	Has the same meaning as in the PPIP Act.
Sensitive information	Information referred to in section 19(1) of the PPIP Act. A special type of 'personal information' (see above). Some of our 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.
Service Partnership Agreement	The agreement Service NSW enters into with partner agencies and organisations, which stipulates the terms, conditions, requirements, specifications, and responsibilities regarding the transactions Service NSW completes on the agency's behalf.

Privacy Management Plan

PART A: Introduction

Introduction to Service NSW and its privacy context

Service NSW was established in 2013. The CEO of Service NSW exercises functions under the *Service NSW (One-stop Access to Government Services) Act 2013* (the Service Act).

Service NSW exercises some functions in its own right, but primarily acts as the 'single front door' for customers to access government services, delivered in partnership with other agencies. The CEO exercises customer service and other functions for partner agencies under delegation or by agreement.

Service NSW provides:

- A single 24/7 NSW Government phone number
- A customer friendly government web portal
- Service centres where multiple transactions are carried out efficiently for customers
- Mobile applications that provide real-time information as customers need it.

Service NSW processes and systems

Service NSW has agreements with around 63 NSW Government partner agencies to facilitate over 1,200 interactions and transactions for the community. Our partner agencies span non-government organisations, and federal, state, and local government levels.

Service NSW adopts a multi-channel model of service delivery entailing 'digital, over the counter and over the phone' services, through 153 points of presence including Service Centres, council agencies, digital self-serve kiosks, Mobile Service Centres, and contact (call) centres. In implementing this multi-channel model, Service NSW uses a range of different IT systems. The nature of the services provided by Service NSW varies across agencies and transactions. Some services are provided wholly by Service NSW, such as the NSW Seniors Card application process and, more recently, various initiatives responding to the COVID-19 pandemic and responses to natural disasters such as the 2019–20 bushfire emergency.

For other transactions, Service NSW staff access the systems of partner agencies to conduct transactions on behalf of those agencies. For example, Service NSW staff in service and contact centres may access the IT system owned by Transport for NSW to enter data for licence and

registration transactions.

Service NSW staff may also access partner agency systems to provide information in response to enquiries. For example, contact centre staff have read-only access to a system owned by the NSW Registry of Births, Deaths and Marriages to answer enquiries over the phone.

In addition to the partner agency systems, staff in contact centres and other head office staff have access to a Service NSW licensed version of Salesforce. Salesforce is a commercial, cloud-based software application primarily used for customer relationship management. Service NSW uses Salesforce for retaining customer account details, to record customer interactions, and to make bookings for matters that require an appointment.

Customer information for some individual programs is also stored on the Salesforce system, as well as the MyServiceNSW account information for over 4.3 million Service NSW customers. In addition, the Service NSW website and MyServiceNSW account feature are also partly hosted on the Salesforce platform. Service Centre staff do not have access to Salesforce, while some staff in partner agencies do have access.

Applicable privacy laws

As a “public sector agency”, the handling of personal and health information by Service NSW is regulated by the NSW privacy laws:

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

The PPIP Act regulates 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 regulates the handling of “health information” by public sector agencies. “Health information” is like 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 agencies 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". These can be found in the two Acts themselves, and in Regulations, Privacy Codes and Public Interest Directions.

Part 2, Division 3 of the PPIP Act contains exemptions that may allow Service NSW to not comply with the IPPs in certain situations. Some examples include:

- Service NSW 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. For example, if information is shared in accordance with the Service Act, this will be lawful, regardless of any IPP that would otherwise apply.
- Service NSW is not required to comply with IPPs with respect to collection if the information concerned is collected for law enforcement purposes. However, this subsection does not remove any protection provided by any other law in relation to the rights of accused persons or persons suspected of having committed an offence.
- Service NSW is not required to comply with the IPPs in relation to the collection, use or disclosure of personal information if it is reasonably necessary to assist in a stage of an emergency, and it is for the purpose of assisting in the stage of the emergency, and it is impracticable or unreasonable to seek the consent of the individual.
- Service NSW is not required to comply with IPP 2 (direct collection) if the information concerned is collected in relation to court or tribunal proceedings.
- Service NSW 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 agencies concerned for example, for the use of corporate services of another agency. However, prior to doing so the

agency will either de-identify 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 agencies), or

- to allow any of the agencies concerned to deal with, or respond to, correspondence from a Minister or Member of Parliament.

Service NSW 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 for the purpose of research, or the compilation or analysis of statistics, in the public interest, and where a direct collection from the individual to whom the information relates is unreasonable or impractical. When doing so, Service NSW takes reasonable steps to de-identify the information or where the information cannot be de-identified ensure that the information is not published in a publicly available publication. Please see Appendix 2 for other general exemptions which Service NSW may rely upon.

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

For example, the public interest 'Direction relating to Service NSW' enabled a time-limited exchange of personal information between Service NSW, Transport for NSW and the NSW Registry of Births, Deaths and Marriages which would otherwise not have been permitted under the PPIP Act. This direction was made on 5 August 2020, to allow Service NSW to obtain up-to-date contact details of customers impacted by the 2020 Service NSW cyber incident, and to determine customers impacted by the 2020 Service NSW cyber incident who are deceased, and the direction expired on 31 January 2021. Currently, there are no directions in operation that Service NSW relies on.

Some agencies will also have a Privacy Code of Practice. This is a document approved by the NSW Privacy Commissioner that provides agencies with specific exemptions from the Information Protection Principles in order to carry out their functions. There are currently no codes of practice that are likely to affect how Service NSW manages personal information. More information on Privacy Codes of Practice is available on the IPC website: https://www.ipc.nsw.gov.au/privacy/nsw-privacy-laws/privacy-codes-practice

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
- employees
- persons conducting a business or undertaking
- insurers
- 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 representatives
- courts and tribunals
- Ministers and Parliament
- NSW partner agencies.

Responsibilities of employees, contractors, and service providers

All employees, contractors and service providers of Service NSW are required to comply with the PPIP and HRIP Acts.

Both Acts contain privacy principles which apply to Service NSW. If the privacy principles are breached, Service NSW may face loss of customer trust, and financial costs including compensation. Both Acts also contain criminal offence provisions applicable to employees, contractors and service providers who use or disclose personal information or health information without authority.

This Plan is intended to assist employees, contractors, and service providers to understand and comply with their obligations under those Acts. If Service NSW employees, contractors or service providers feel uncertain as to whether certain conduct may breach their privacy obligations, they should seek the advice of the Service NSW Privacy Officer.

Employees, contractors, or service providers who are suspected of conduct which would breach the privacy principles or the criminal provisions may be disciplined as for a breach of the Code of Conduct. Suspected criminal conduct may result in dismissal 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.

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 Service NSW (including former employees and contractors) to intentionally use, disclose or offer to supply 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.

It is also 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 Data Breach

Service NSW, upon becoming aware of a data breach which involves personal or health information and 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 customers who may be at risk of suffering serious harm.

Privacy Management Plan

Privacy Officer for Service NSW

Risk Strategy and Performance Division, Service NSW
GPO Box 7057, Sydney NSW 2001
Phone: 13 77 88
Web: www.service.nsw.gov.au/privacy
Email: privacy@service.nsw.gov.au

The Department of Customer Service (DCS), a central department in the NSW Government, has over 30 agencies, entities, and business units, including Service NSW, which is an executive government agency related to DCS.

Risk, Strategy and Performance

The Service NSW Risk, Strategy and Performance (RSP) business unit has responsibility for managing Service NSW's privacy management functions, including internal privacy reviews. RSP works together with DCS to obtain relevant privacy management and policy advice.

Responsibilities of the Privacy Officer

The Service NSW Privacy Officer leads a team that is responsible for:

- ensuring the PMP remains up to date
- publishing the PMP
- informing employees and contractors of any changes to the Plan
- making a range of guidance material available to Service NSW employees, contractors, and service providers to help them understand their privacy obligations, and how to manage personal and health information in their everyday work
- providing 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
- recommending controls to help manage privacy risks, and providing privacy expertise to assist their implementation
- responding to privacy incidents
- handling privacy complaints

- maintaining reporting on privacy incidents, complaints, and other relevant metrics
- providing privacy training and awareness activities to Service NSW employees, contractors, and service providers, and
- being available to answer any questions Service NSW employees may have about their privacy obligations.

In carrying out these responsibilities, the Service NSW Privacy Officer may work with the DCS Privacy Officer, and partner agencies' privacy officers, where appropriate.

The Privacy Officer, in accordance with clause 6 of the *Annual Reports (Departments) Regulation 2015,* is to ensure that the Service NSW Annual Report includes:

- a statement of the actions taken by Service NSW in complying with the requirements of the PPIP and HRIP Acts, and
- statistical details of any internal reviews conducted by or on behalf of Service NSW.
- The Privacy Officer is to review and update this PMP:
    - if Service NSW wishes to introduce a significant new collection of personal information, or
    - 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 Service NSW, or
    - at the conclusion of the 2021-22 reporting year.

Service NSW, 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 website and the Service NSW intranet 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 Service NSW 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 (see sections on access, correction and complaints below).

Privacy Management Plan

PART B: Service NSW and its partner agencies

Transactions that Service NSW performs

Under the Service Act, Service NSW exercises customer service functions on behalf of other NSW Government agencies, Local Government, and some private sector organisations.

The most common transactions performed by Service NSW include:

- accepting applications for and processing licences, permits and authorities, such as driver licences, car registration, boating and fishing licences on behalf of Transport for NSW
- management of the toll relief scheme
- receiving applications for the registration of births, deaths, and marriages
- requests for replacement certificates or other documents to be issued by the Registrar of Births Deaths and Marriages
- receiving fines and taxes on behalf of Revenue NSW,
- applications for Fair Trading and Safe Work permits, certificates and authorities, and
- processing applications for Working with Children Checks for the Office of the Children's Guardian.

Service NSW also administers grants and vouchers on behalf of the NSW Government. This includes grants to small business and individuals affected by emergencies such as bushfires and floods, and return to work grants which are aimed at women who are victims/survivors of domestic and family violence. Service NSW provides vouchers on behalf of other NSW Government agencies to individuals to use with organisations and businesses. This includes:

- Active Kids
- Creative Kids
- First Lap
- Before and After School Care
- Dine and Discover Vouchers
- Stay and Rediscover
- Parent Vouchers

Service NSW has assisted the response to the COVID-19 pandemic by providing various support measures on behalf of the NSW Government. This includes COVID-19 specific grants for

businesses affected by the COVID-19 pandemic such as the COVID-19 Micro and Small Business Grants, COVID-Accommodation Support Grant, and COVID-19 Job Saver Payments. COVID-19 initiatives that are delivered to the wider community are detailed further on page 17.

To conduct transactions, Service NSW collects personal and health information. This information may be collected to meet the legal requirements of the transaction concerned, to prove the identity of the customer, or in connection with payments. The information may include name, address, date of birth, names of family members, passport details, qualifications, and medical information or certificates. Financial information may also be collected for payment purposes.

Personal and health information may be collected:

- over the counter in service centres to ensure there is a record of proof of identity, taking photographs for licence renewal or conducting vision tests for driver's licences
- through the Service NSW Contact Centre, such as the retention of phone call records and written records of customer requests and information prepared by staff; and
- through information provided by customers for online transactions (including using the Service NSW app).

Personal and health information may be held in Service NSW systems. Personal and health information may also be transmitted to partner agencies and organisations.

Disclosure of personal and health information collected by Service NSW and its partner agencies is governed by specific statutory authorisations in various legislation (such as legislation administered by Transport for NSW) and consents which are completed by customers.

Service NSW is bound by the requirements of the *State Records Act 1998* in relation to the retention of personal and health information.

Agreements are in place with partner organisations requiring that both Service NSW and partner organisations adhere to the requirements of the privacy legislation and their own statutory schemes in the collection, storage, retention, and disclosure of personal and health information. These agreements are reviewed to ensure that the respective privacy obligations of Service NSW and partner organisations are adequately documented.

Service NSW holds personal and health information both (a) in its own right, and (b) when exercising customer service functions for another agency.

Information held in its own right

Information that Service NSW holds in its own right includes:

- Information collected when exercising functions relating to the delivery of government services to the people of New South Wales as directed by the Minister, under s. 4(c) of the Service Act
- Information collected for the purpose of setting up and using MyServiceNSW accounts, and
- Information collected for the purpose of exercising employer functions, including personal information of its employees and contractors.

Information held when exercising functions for partner agencies

Service NSW exercises customer service functions under delegation or by agreement for other NSW government agencies, the Commonwealth, other state and territory governments and some non-government entities. Service NSW refers to these other entities as “partner agencies”.

Internal records

Service NSW may collect, maintain and use, for the purpose of its interactions with customers for whom relevant functions are exercised, details of transactions between customers and Service NSW, the preferences of customers for transacting matters and receiving information from Service NSW and the agencies for which it acts and other information about customers: Service Act, s. 11.

Service NSW is responsible for any customer data which it maintains for internal administrative purposes, as well as customer data collected into or via the Salesforce system, in Office 365 applications and online.

MyServiceNSW

MyServiceNSW is an online service run by Service NSW which has been developed to make it easier to perform transactions with NSW government agencies online. A MyServiceNSW Account is an electronic profile that a customer can use to store personal information and enable electronic transactions that require identity verification.

Creating a MyServiceNSW Account is voluntary. Service NSW collects personal information from customers in order to create a MyServiceNSW account, to pre-complete online forms, and to

complete and store information relevant to transactions the customer has performed, or products that the customer holds, such as a driver licence or vehicle registration.

COVID-19 initiatives supported by Service NSW

Service NSW supports the community during the COVID-19 pandemic by delivering a number of services and initiatives. Below is a summary of the active COVID-19 initiatives currently supported by Service NSW:

COVID Safe Check-in

Service NSW provides and electronic registration tool called the COVID Safe Check-in. This allows customers, staff and visitors to check in at businesses across NSW, and meet requirements for the quick and accurate collection of customer contact details as required under Public Health Orders.

Service NSW collects personal information from customers when they use either the COVID-19 Safe Check-in tool via the Service NSW app or using the Service NSW Web Check-in function. Service NSW collects customers' contact details and creates a record of their attendance at a venue for the purposes of registering that attendance in accordance with Public Health Orders made under section 7 of the *Public Health Act 2010*. This is to help protect the health and welfare of members of the public during the COVID-19 pandemic, including so that customers can be contacted by NSW Health in the event that another person at that venue is a confirmed or suspected case of COVID-19.

Service NSW can send advisory notifications and advice to customers, on behalf of NSW Health, if they might be at increased risk of becoming infected. The information is kept for a period of 28 days from the date it was collected and provided to the Chief Health Officer, if requested, for contact tracing purposes. Upon expiry of the 28 days from collection, the personal information is permanently deleted.

COVID-19 digital certificate

Individuals can elect to use their Service NSW app to show proof that they are vaccinated against COVID-19. Individuals can choose to share their COVID-19 vaccination certificate with Service NSW through Services Australia. Service NSW will only collect COVID-19 vaccination certificate information from Services Australia with consent. Service NSW will use your COVID-19 vaccination

certificate information, including your ongoing vaccination status, to create a digital copy of your COVID-19 vaccination certificate in the Service NSW app on your device. This forms part of the check-in information Service NSW holds about you.

COVID-19 wellbeing response

Service NSW collects personal information from individuals to assist them in accessing programs or services that may help them through the COVID19 pandemic. We use and disclose this information to connect individuals with the Australian Red Cross and Resilience NSW to check on their wellbeing and provide essential support and services.

Register a positive COVID-19 rapid antigen test result

People in NSW who obtain a positive COVID-19 test result using a rapid antigen test must register their details with Service NSW. Service NSW collects personal and health information to enable NSW Health to provide individuals with information about care, treatment, and access to health and hospital services when appropriate. NSW Health also uses information collected to monitor numbers and locations of COVID-19 cases across NSW.

Personal and health information collected by Service NSW will be shared with NSW Health. Personal and health information collected in the registration form is temporarily stored by Service NSW. All stored information will be transferred to NSW Health prior to deletion.

NSW Health Pathology Notifications

Individuals that opt-in can choose to receive information about their COVID-19 result from Service NSW via SMS or email. Service NSW collects your personal and health information to send you notifications about NSW Health Pathology COVID-19 results on behalf of NSW Health.

Inactive COVID-19 initiatives

Service NSW has handled personal and health information through other initiatives that have supported the COVID-19 pandemic in the past. These initiatives are no longer active and included:

- COVID-19 Nominated Visitor Register and the COVID-19 Travel Registration
- COVID-19 Test and Isolate Payment
- Interstate and International Border Entry Declarations

COVID-19 information protected under the Service Act

The *Service NSW (One-stop Access to Government Services) COVID-19 Information Privacy Amendment Bill* was passed in 2021. These amendments ensure that personal and health information collected by Service NSW under the Public Health Orders cannot be used or disclosed except in very limited circumstances. The amendments prevent Service NSW from disclosing personal and health information collected under the Public Health Orders for any use other than:

- the purpose for which it was collected
- contact tracing, including in another Australian jurisdiction
- to provide access to the person it is about
- or in limited circumstances to investigate a breach of the Public Health Orders when it relates to the issue of a permit or a border declaration.

Cyber Incident Helpline

Service NSW has been engaged to operate a dedicated Cyber Incident Helpline to provide resources for managing inbound calls on behalf of NSW Health and the Department of Education. Whilst undertaking the call centre function, SNSW obtains proof of identification from customers to provide further information and support to those people impacted by cyber incidents. The information available to call-takers may include the risk category the file and person belong to, and contextual information about what the files containing personal information may have been impacted. Service NSW will only use or disclose the information to the agencies for the purposes of supporting customers and enabling those agencies and their service providers to further manage the incident. At the conclusion of the Service NSW support services, all information disclosed to or collected by Service NSW will be securely transferred to NSW Health or the Department of Education after which Service NSW will not retain the information.

Updating customer information with other agencies

Service NSW can disclose information about a person that is obtained in the course of providing a relevant function to that person to another government agency, but only if the person consents to the disclosure of the information to that other agency: Service Act, s. 6.

Where Service NSW performs a transaction for a customer in its own right, it will ask the customer for consent before sharing that information with a different agency.

Relationship with partner agencies

Most customer personal information Service NSW handles is for the purpose of fulfilling a transaction on behalf of a partner agency. Service NSW may collect and hold personal and/or health information when exercising functions for the agencies listed in Appendix 4.

Service NSW will update this PMP periodically to update this list of partner agencies.

Where Service NSW exercises functions for a partner agency, Service NSW is responsible for complying with its privacy obligations in terms of the personal information that is collected, stored and processed on behalf of that agency, including ensuring data security and data quality. Service NSW can share information it obtains with the partner agency, without separately requesting the customer's consent. This is consistent with Service NSW being a shopfront for the partner agency. Service NSW can also share the information it obtains with any person the partner agency is authorised or required to disclose the information to.

The Service NSW Privacy Statement provides more information on how Service NSW handles personal information including how to seek access to personal information. The Service NSW Privacy Statement also includes links to relevant partner agency Privacy Collection Notices or Statements to provide more information on those agency's information handling practices.

Respective privacy obligations of Service NSW and partner agencies

Depending on the circumstances, Service NSW and a partner agency may both have privacy obligations in respect of the same information. For example, where Service NSW has access to a partner agency's information system, both Service NSW and the partner agency are required to protect the information against unauthorised access, and both are generally prohibited from disclosing it.

In practice, Service NSW will determine how to comply with its privacy obligations in collaboration with its partner agencies. In particular:

- when exercising functions for a partner agency, Service NSW will only handle personal and health information in accordance with any relevant instrument of delegation or agreement, and
- partner agencies may specify matters such as the applicable retention periods, security requirements and contents of privacy collection notices.

Privacy Management Plan

Service NSW as a cluster agency

NSW Government departments, agencies and organisations are arranged into nine groups, called clusters. Service NSW is an executive agency related to the Department of Customer Service, and therefore within the Customer Service cluster.

Clusters have no legal effect for privacy purposes. Service NSW must comply with the applicable privacy principles. Where Service NSW uses personal or health information internally, this will constitute a “use” principle for privacy purposes. Where Service NSW provides information to another person or body, including another agency within the Customer Service cluster, this will constitute a “disclosure” principle for privacy purposes.

Service NSW employees should be aware that there is no special provision for giving personal or health information to other agencies within the Customer Service Cluster. Care should be taken to ensure that any such disclosure complies with applicable privacy requirements. If you are not sure, check with the Service NSW Privacy Officer.

Service NSW may disclose personal or health information to a Customer Service Cluster agency in circumstances including:

- while seeking legal advice, where legal services are provided by DCS
- to enable inquiries to be referred between the agencies concerned
- under a delegation to enable DCS to exercise employee functions, or
- where the disclosure is reasonably necessary for law enforcement purposes, including the investigation of suspected fraud.

Verification of proof of identity

Service NSW will often request a customer to provide proof of identity. Proof of identity may be required in order to proceed with a particular transaction.

Service NSW may use a verification service such as the Commonwealth document verification service. Service NSW will not disclose proof of identity information to a verification service, or obtain the results from a verification service, without first obtaining the customer’s authority, unless there is some other legal basis for doing so.

Service NSW may collect proof of identity information in its own right, or as part of a transaction for a partner agency.

PART C: Types of personal and health information held

Due to Service NSW's diverse role, the type of personal and health information held is also 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 ('customer records'), and
- personal and health information about our staff ('employee and contractor records').

Customer records

These are records relating to our customers or the customers of our partner agencies. Service NSW interacts with customers through three different channels: either a Service Centre (face to face), Contact Centre (by phone) or online (website, live chat, Service NSW app, social media, or other digital facility). These interactions will fall within one of the customer service functions conferred on the CEO of Service NSW under the Service Act.

The main types of customer personal information that we collect and hold are:

- Identity, demographic and contact data such as name, address, telephone numbers and email address, date of birth, gender, and signature.

The main types of customer health information that we collect and hold are:

- Information about physical or mental health or disability provided in applications for licences, permits and other authorities
- Identity, demographic and contact data such as name, address, telephone numbers and email address, date of birth, gender and signature collected by a partner agency that provides a health service, such as COVID-19 testing.

Employee and contractor records

The types of personal and health information held by Service NSW and its delegates about its employees and contractors include:

- identity, demographic and contact data such as name, address, telephone numbers and email address, date of birth, gender, and signature
- 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.

People and Culture

An employee of Service NSW may access their own personnel file without cost. Apart from the employee the file relates to, People and Culture staff, nominated GovConnect staff and any other authorised delegates that have authorised access to personnel files.

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

Managers

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

Self-service function

Service NSW employees and contractors have access to some soft copy records contained in Service NSW's enterprise business software used for managing employee and contractor information. This means staff have direct access to view and edit information, including applying for leave, viewing pay details, updating bank details, address, and email.

GovConnect

Day to day human resource operations of most staff, are conducted under an outsourced arrangement called GovConnect. 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 protect employees' personal information.

Therefore, GovConnect holds and is responsible for some personal information such as recruitment, work arrangements, payroll and leave records. The Service Partnership Agreement between Service NSW and GovConnect notes that GovConnect will have access to information from and about Service NSW in the course of business, and that GovConnect is bound to comply with the privacy laws.

Other information

Service NSW may also hold other miscellaneous personal and health information such as information contained in correspondence with members of the public (other than in relation to the performance of customer service functions).

PART D: How the privacy principles apply

Important note about using this Part

This part of the PMP uses plain language, not the exact wording of the law to describe the privacy principles and how Service NSW employees and contractors will comply with them. This is to make understanding our obligations easier. This document does not cover the full complexity of the privacy laws applying to Service NSW. It has been simplified and does not cover all exemptions or situations. If in doubt, you should always check the exact wording in the legislation, and seek guidance from the Service NSW Privacy Officer, or the NSW Privacy Commissioner. This document is an educational tool, not legal advice.

Introduction

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.

Our privacy obligations have been condensed into one set of 12 plain language principles to be followed by Service NSW as follows (references in brackets are to the principles in the PPIP and HRIP Acts):

- limiting our collection of personal information (IPP 1 and HPP 1)
- anonymity and identifiers (HPPs 12 and 13)
- how we collect personal information – the source (IPP 2 and HPP 3)
- how we collect personal information – the method and content (IPP 4 and HPP 2)
- notification when collecting personal information (IPP 3 and HPP 4)
- security safeguards (IPP 5 and HPP 5)
- transparency (IPP 6 and HPP 6)
- access (IPP 7 and HPP 7)
- correction (IPP 8 and HPP 8)
- accuracy (IPP 9 and HPP 9)
- use (IPP 10 and HPP 10)
- disclosure (IPPs 11 and 12, and HPPs 11, 14 and 15).

The PMP outlines key definitions, and for each of the plain language privacy principles:

- a summary description
- when there are different rules for ‘sensitive’ or ‘health’ information
- some key points about how the privacy principles work in practice in the context of Service NSW’s functions, and
- any relevant exemption.

This part of the PMP relates mainly to the way in which Service NSW handles customer records.

The Privacy Principles

1. Limiting our collection of personal information (IPP 1 and HPP 1)

1.1. The principle in brief

We will only collect personal 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 acquire information in many different ways. Examples include: a written form, a verbal conversation, an online form, a voice recording or taking a picture or image.

We won’t ask for personal information unless we need it to perform one of our customer service functions, for the purpose of updating contact details with an individual’s consent, or for internal administrative purposes. We will especially avoid collecting sensitive information if we don’t need it.

Often our partner agencies are responsible for defining what customer information is needed to fulfil a transaction. Where we exercise a customer service function for a partner agency, we will only collect information that the partner agency could collect if it was performing the function itself.

In other circumstances, we ensure that only the minimum required information is collected or recorded to fulfil our customer service functions.

2. Anonymity and Unique Identifiers (HPP 12, 13 and 15)

2.1. The principle in brief

We will allow people to receive services from us anonymously, where lawful, secure, and practicable. We will only assign identifiers (such as customer numbers) to customers where required to do so by our partner agency.

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

2.2. How we apply this principle

People making informal enquiries or requesting general information, should not be required to identify themselves.

Service NSW takes care not to inadvertently collect customers' health information. When this type of information is collected, it is not given any separate identifier and it is not included in any health records linkage system.

People & Culture may collect health information 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, it is held against the investigation file, and not given any separate identifier. People and Culture have no linkages to any health records systems.

3. How we collect personal information – the source (IPP 2 and HPP 3)

3.1. The principle in brief

A government agency may disclose information to Service NSW so that Service NSW can exercise customer service functions for the agency or other related functions: Service Act, s. 14(4). In these circumstances, customers' consent is not required, and Service NSW does not have to collect the information directly from the individual. This is consistent with Service NSW being a shopfront for the partner agency.

Apart from that, we collect personal information directly from the person unless they have

authorised otherwise or, in the case of health information, it would be unreasonable or impractical to obtain the information directly from the person.

3.2. How we apply this principle

Some of Service NSW's customer service functions will relate to transactions that require exchange or verification of personal information with third parties. Collection from a third party should be authorised by the individual, unless there is some other basis for not complying with this requirement (for example, if the particular statutory scheme contemplates that the information be collected from a third party).

Compliance with this principle will largely be the responsibility of partner agencies, effected through the procedures included under Service Partnership Agreements.

Collection of personal information by Service NSW for its own internal administration purposes should not require collection via third parties. By collecting information directly from the source, it is easier for us to comply with other obligations too, like ensuring the accuracy of the information, and getting permission for any secondary use or disclosure of the information.

3.3. Other considerations

Where a person is under 16, we may collect their personal information from their parent or guardian. Where a person aged 16 or over has limited capacity (e.g. because of mental illness, intellectual disability, dementia, brain injury, illness, accident or disease), we can ask their authorised representative for the information instead. However, we may also communicate with them directly. The NSW Privacy Commissioner's guide *Privacy and People with Decision-making Disabilities* explains how to collect personal information from or about a person who has limited or no capacity.

The NSW Privacy Commissioner's *Handbook to Health Privacy* provides some other examples of when it might be "unreasonable or impractical" to collect health information directly from the person.

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

4.1. The principle in brief

- We will not collect personal information by unlawful means
- We will not collect personal information that is intrusive or excessive

- We will ensure that the personal information we collect is relevant, accurate, up-to-date, complete, and not misleading.

4.2. How we apply this principle

Service NSW will take reasonable steps to ensure that collection is lawful. The types of personal information collected in the Service Centre and Digital channels are defined for us by our partner agencies. In our Contact Centre, employees who record information from callers must be mindful of this principle, and only record in Salesforce the minimum information necessary to provide the service requested.

Inbound calls to the Service NSW Contact Centre will normally be recorded for the purpose of quality and training purposes. Notice of call recordings is provided to the callers, however, callers cannot elect for their call to not be recorded (see 5 below).

Recording with prior notice complies with the participant monitoring provisions of the *Telecommunications (Interception and Access) Act 1979* (Cth) as well as NSW privacy and surveillance laws.

Ensuring that personal information is of high quality is a constant challenge, particularly given the range of transactions that Service NSW performs. However, it is reasonable to assume that individuals using Service NSW will generally give us information that is 'fit for purpose', and regular customer contact provides an opportunity to check accuracy of data with individuals, where that is appropriate. Where appropriate, Service NSW uses automated techniques so that details such as addresses and telephone numbers are recorded in the correct format.

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. Personal and health information may also be collected directly from the staff member within a business unit 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.

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

5.1. The principle in brief

When collecting personal information, we will take reasonable steps to inform the person of:

- who holds and/or has access to their personal information
- what it will be used for
- which organisations (if any) routinely receive this type of personal information from us
- if the collection is required by law
- what the consequences are for the person if they do not provide the information to us, and
- how the person can access their personal information held by us.

5.2. How we apply this principle

Where Service NSW collects personal information in its own right, including for its own internal administrative purposes, it will make customers aware of the specified matters. We will do this through a variety of channels, including pre-recorded voice messages and printed and online notices. Service NSW adopts a layered approach to privacy notices, as endorsed by the Privacy Commissioner, to avoid overloading customers with too much information. A concise basic notice will meet legislative obligations as a minimum and will include information about how to obtain more detail if desired.

Where we exercise customer service functions on behalf of a partner agency, we will either provide the customer with a privacy notice supplied or endorsed by the partner agency (e.g. on partner agency paper or online forms, or in relevant telephone scripts), or will refer the person to information provided by a partner agency in relation to the collection of the information.

5.3. Other relevant points

A *Guide to Drafting Privacy Notices* is attached in Appendix 3 to this document. This can be used as the starting point for staff who are drafting notices to be delivered through different channels.

The Service NSW Privacy Officer should review any proposals to collect new personal information or to use existing personal information for a new purpose, to ensure an adequate privacy notice is included.

Privacy collection notices should be specific. If information is being collected for more than one purpose, each purpose for which the information is being collected should be specified.

A privacy collection notice is not a request for consent. Its function is to tell the person providing the

information of the specified matters.

For Non-English-speaking customers, the NSW Privacy Commissioner's *Community Language Privacy Notice* should be used. The NSW Privacy Commissioner's guide *Privacy and People with Decision-making Disabilities* explains how to notify a person who's decision making capacity is impaired by a range of conditions including mental illness, intellectual disability, dementia, brain injury or stroke.

In the case of inbound calls to the Contact Centre, a recorded message will give notice that the call may be recorded or monitored. Contact Centre employees making outbound calls must provide the notice themselves

6. Security safeguards – storage of personal and health information (IPP 5 and HPP 5)

6.1. The principle in brief

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

6.2. How we apply this principle

Retention and disposal

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.

Where Service NSW holds information in its own right, Service NSW is wholly responsible for ensuring that information is kept for no longer than necessary. Where Service NSW exercises functions for a partner agency, Service NSW will dispose of information securely in accordance with any retention period specified by the partner agency.

Security safeguards

Service NSW will protect information by implementing security safeguards as are reasonable in the circumstances against loss, unauthorised access, use, modification or disclosure, and against all

other misuse, whether it holds the information in its own right or in the exercise of functions for a partner agency.

Where Service NSW exercises functions for a partner agency and holds or has access to personal or health information in that capacity, Service NSW is responsible for complying with requirements relating to storage and security of personal and health information in consultation with the partner agency. The partner agency may specify what security safeguards are required.

Security measures include technical, physical and administrative actions.

All employees, including contractors, are required to comply with the Service NSW *Code of Conduct* and Service NSW *Information Security Policy*. The *Information Security Policy* sets out the actions Service NSW takes to secure information, including maintaining an Information Security Management System compliant with ISO27001:2013. For more information about how we champion information security, refer to the *Information Security Policy*.

Security is considered in data transmission arrangements (including encryption where appropriate), backup and storage. Generally, once data is entered into the secure system, any paper documents are shredded or destructed securely so that they cannot be accessed inappropriately.

Service NSW applies disposal schedules in accordance with the *State Records Act 1998.* In business units that deal with substantial amounts of private or sensitive information, such as human resource units or investigation teams, access to the floor or the room where personal information is stored may be restricted to authorised personnel.

7. Transparency (IPP 6 and HPP 6)

7.1. The principle in brief

Once a person has confirmed their identity, will we take reasonable steps to allow them to find out:

- whether we are likely to hold their personal information
- the nature of the information we hold
- the purposes for which we use personal information, and
- how a person can access their own personal information.

7.2. 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 a collection notification, which is more specific, and given to customers at the time of collecting new personal information.

This PMP will be accessible through our website. It sets out the major categories of personal information that we hold and explains our privacy obligations.

A schedule of our partner agencies, with whom we share customer personal information, is attached at Appendix 4.

For more information, contact the Service NSW Privacy Officer.

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

8.1. The principle in brief

We will allow people to access their personal 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.

8.2. How we apply this principle

Where individuals seek access to information we hold about them in relation to a transaction with a partner agency, we will normally refer them to that agency to process their request, unless the relevant Service Partnership Agreement with that partner agency has provided for us to do this on their behalf.

Many customer service requests processed by Service NSW on behalf of partner agencies could be construed incidentally as requests for personal information, e.g. ‘Is my licence current? What are the conditions of my permit?’ Such requests will be handled in accordance with specifications set out in the Service Partnership Agreement with the relevant agency, rather than treated as access requests under either the PPIP, HRIP or GIPA Acts.

People (whether customers, employees or other individuals) should generally be able to see what information Service NSW holds about them with a minimum of fuss. Requests can be made by phone, email or in person. Access to your own information is free.

8.3. Exemptions

Before relying on an exemption, Service NSW employees and contractors should check with the Service NSW Privacy Officer.

In some circumstances, another law may prevent us from giving the person access to the information requested.

8.4. Other relevant points

The NSW Privacy Commissioner's guide *Privacy and People with Decision-making Disabilities* explains how to provide access to personal information held about a person who has limited or no capacity. Formal access applications under the PPIP Act will be handled by the Service NSW Privacy Officer or equivalent authorised personnel. Formal access applications under the GIPA Act are handled by the dedicated GIPA team for Service NSW.

If there is any doubt about whether a request to personal information is from the individual to whom the information relates or their authorised representative, the request should be referred to the Service NSW Privacy Officer or equivalent authorised personnel.

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

9.1. The principle in brief

We will allow people who have confirmed their identity to update or amend their personal information, to ensure it is accurate, relevant, up-to-date, complete, or not misleading.

9.2. How we apply this principle

For Service NSW, correction of customer information is part of our customer service functions. We will actively encourage and remind customers to keep any information we hold about them accurate, up to date and complete, to the extent that they wish to do so.

When an individual requests a change to their contact details, either in relation to a specific transaction or more generally, Service NSW may offer them choices in respect of updating information held by other government agencies.

If the relevant record is controlled by a partner agency and not by Service NSW, we may refer you

to the partner agency so that you can ask the partner agency to correct your information.

If we disagree with an individual about whether the information needs changing (for example if we have determined that the information held is an accurate record), we can decline to do so, but must instead allow the person to add a statement or notation to our records. We cannot charge individuals for requesting for amendment, or for processing such a request or for making an amendment.

Requests by Service NSW employees for changes to personnel records will be processed in accordance with relevant HR policies.

9.3. Exemptions

Before relying on an exemption, Service NSW employees and contractors should check with the Service NSW Privacy Officer. We can decline to make an amendment if another law authorises or requires us not to do so, although the correction right in privacy laws overrides 'non-alteration' provisions of the *State Records Act 1998.*

9.4. Other relevant points

If there is any doubt about whether a request for amendment of personal information is from the individual to whom the information relates (or their authorised representative), or it there are any doubts about such a request, the request should be referred to the Service NSW Privacy Officer.

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

10.1. The principle in brief

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

10.2. How we apply this principle

Service NSW will take such steps as are reasonable in the circumstances to ensure that the information is relevant, accurate, up to date and not misleading.

For most of Service NSW's functions, checking information before use or disclosure will be 'built in'

to normal operating procedures, e.g. asking customers to verify their personal information while processing a transaction.

What might be considered “reasonable steps” will depend upon 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 the person if the information is inaccurate or irrelevant
- any opportunities we’ve already given the person to correct inaccuracies, and
- the effort and cost involved in checking the information.

Where Service NSW is exercising functions for a partner agency, it is reasonable, having regard to the purpose for which the information is proposed to be used, for Service NSW to rely on the steps taken by the partner agency to ensure that the information is accurate, before Service NSW uses it.

If Service NSW receives information from a third party that your details have changed, we will contact you to verify the information with you prior to amending your information.

11. Use – how we use personal and health information (IPP 10 and HPP 10)

11.1. The principle in brief

Service NSW uses information when it employs the information internally for some purpose or gives it to a contractor.

We may use personal information:

- for the primary purpose for which it was collected, or
- for a directly related secondary purpose, or
- if Service NSW reasonably believes that the use is necessary to prevent or lessen a serious and imminent threat to life or health, or
- for another purpose if the person has consented.

11.2. How we apply this principle

Customer information

A partner agency may disclose information to Service NSW so that Service NSW can exercise functions for the partner agency. Service NSW can use the information for that purpose: Service Act, s. 14(4) and (6).

As a general principle, we use the personal and health information we've collected only for the purpose for which it was collected, as set out in the privacy notice for that particular service. The primary purpose for which we use customers' personal information will be one or more of our customer service functions.

We may also use information for directly related secondary purposes such as auditing, reporting or program evaluation. For example, if the primary purpose of collecting a complainant's information was to investigate their customer complaint, then independent auditing of our complaint-handling practices would be an acceptable use for a directly related secondary purpose.

With consent, we may also use a customer's personal information for updating their contact information with other agencies.

To use personal information for any other purpose, Service NSW employees and contractors should check with the Service NSW Privacy Officer first.

The NSW Privacy Commissioner's guide *Privacy and People with Decision-making Disabilities* explains how to seek consent for a secondary use of personal information from a person who has limited or no capacity. The NSW Privacy Commissioner's *Statutory Guidelines on Research* explain how health information can be used for research purposes. It also provides a good rule of thumb for the use of other types of personal information for research purposes.

Employee information

If you are a Service NSW 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 personal information that is held by the agency through SAP and MyCareer. This includes your pay slips, leave balances, comments from your supervisor, timesheets, and other types of personal information. You are also entitled to access your 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 business unit 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 staff 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.

11.3. Exemptions

Service NSW will generally use information with the consent of the person it relates to. However, Service NSW may use personal information without consent in some circumstances, including:

- if another law authorises, requires, implies, or reasonably contemplates the use
- for some law enforcement and investigative purposes (for example, to investigate suspected fraud), or
- for some research purposes, subject to approval by a Human Research Ethics Committee.

In many circumstances, Service NSW will handle information in accordance with the information handling provisions set out in the Service Act, which may differ from the privacy requirements that usually regulate information handling by agencies. This is consistent with Service NSW being a shopfront for its partner agencies.

Service NSW employees and contractors should check with the Service NSW Privacy Officer before relying on an exemption.

12. Disclosure – how we disclose personal and health information (IPP 11 and HPP 11)

12.1. The principle in brief

Service NSW discloses information when it reveals the information to a person or body outside Service NSW who did not previously know the information.

Under privacy law, we may disclose personal information if

- the person has consented, or

- the information is not ‘health information’ or ‘sensitive information’, and the individual has been made aware that the information is likely to be disclosed to the recipient, or
- the information is not ‘health information’ or ‘sensitive information’, and the disclosure is directly related to the purpose for which the information was collected, and Service NSW has no reason to believe that the individual concerned would object to the disclosure, 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 the person’s reasonable expectations.

In addition, we may disclose information in accordance with the information handling provisions set out in the Service Act.

When exercising functions for a NSW Government partner agency, we may disclose information to that government agency, the customer, or any other person to whom the government agency is authorised or required to disclose the information.

When exercising functions for a partner agency other than a NSW government agency, we may disclose information if permitted under the delegation or agreement that confers the power to exercise the function and, in the case of a partner agency that is an agency of the Commonwealth or of another State or Territory, the disclosure is permitted under a law that applies to the exercise of that function.

Service NSW can disclose information obtained in the course of providing functions to that person to another Government agency, with the person’s consent.

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

Under privacy law, disclosing sensitive information (e.g. your ethnic, racial origin, political opinions, religious or philosophical beliefs, trade union memberships or sexual preference) is only allowed with your consent or if there is a serious and imminent threat to a person’s life or health.

We can only transfer ‘health information’ outside of NSW (including to the Commonwealth Government), if one of the following applies:

- the person concerned has consented
- it is necessary for a contract with (or in the interests of) the person concerned
- it will benefit the person concerned, we cannot obtain their consent, but we believe the

person would be likely to give their consent
- we reasonably believe that the recipient of the information is subject to a law or binding scheme equivalent to the HPPs, or
- we have bound the recipient by contract to privacy obligations equivalent to the HPPs.

However, we may disclose information in accordance with the information handling provisions set out in the Service Act, even where this does not comply with requirements under privacy law that would otherwise apply. This is consistent with Service NSW being a shopfront for its partner agencies (which may include other NSW government agencies, the Commonwealth, other state and territory governments and some non-government entities).

12.3. How we apply this principle

Most disclosures made by Service NSW in the course of undertaking its customer service functions or updating customer information with other agencies will be not only 'related' to the primary purpose and within the individual's reasonable expectations but also explained in a privacy notice – meeting two of the conditions in the disclosure principles.

Disclosure of personal information about a customer to the partner agency on whose behalf Service NSW is operating is authorised by s. 14 of the Service Act.

Disclosures for any other purpose need to be tested against the exemptions, outlined below. Before disclosing personal information for any other purpose, or if in doubt, Service NSW employees and contractors should check with the Service NSW Privacy Officer. Requests for personal information from outside bodies, including from government agencies which are not partner agencies of Service NSW, and from partner agencies for information unrelated to the functions Service NSW is performing for them, should be referred to the Service NSW Privacy Officer to assess whether an exemption applies.

12.4. Exemptions

Before relying on an exemption, Service NSW employees and contractors should check with the Service NSW Privacy Officer.

Under privacy law, Service NSW may disclose personal information without consent in some circumstances:

- if we reasonably believe that the disclosure is necessary to prevent or lessen a serious and imminent threat to life or health
- if it is ‘health information’, and we reasonably believe that the disclosure is necessary to deal with a serious threat to public health or safety
- if another law authorises, requires, implies, or reasonably contemplates the disclosure
- if a subpoena, warrant or 'notice to produce' requires us by law to disclose the information
- some research purposes, subject to approval by a Human Research Ethics Committee
- exchanges of information which are reasonably necessary to allow agencies to deal with or respond to correspondence from Ministers or Members of Parliament, or to refer inquiries between agencies, or
- for some law enforcement and investigative purpose (for example, to investigate suspected fraud).

12.5. Other relevant points

The NSW Privacy Commissioner’s guide *Privacy and People with Decision-making Disabilities* explains how to seek consent for a disclosure of personal information from a person who has limited or no capacity. The NSW Privacy Commissioner’s *Statutory Guidelines on Research* explain how health information can be disclosed for research purposes. It also provides guidance on the disclosure of other types of personal information for research purposes.

When the principles do not apply

In certain scenarios the Information Protection Principles and Health Privacy Principles do not apply.

General

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 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
- information sent between public sector agencies to transfer enquiries or to manage correspondence from a Minister or member of Parliament.

The Australian Criminal Intelligence Commission

Where necessary, Service NSW also undertakes police checks with the Australian Criminal Intelligence Commission. In undertaking these checks, we ensure that all personal information collected and received for the purposes of police checks are managed in accordance with our privacy obligations as well as contractual obligations we have with the ACIC.

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 de-identify it so that no person can be identified or otherwise 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 and 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.

Privacy Management Plan

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

Privacy legislation

- *Privacy and Personal Information Protection Act 1998 (NSW)* (PPIP Act)
- *Health Records & Information Privacy Act 2002 (NSW)* (HRIP Act)
- *Privacy and Personal Information Protection Regulation 2014*
- *Health Records and Information Privacy Regulation 2017*
- Codes of Practice, Directions and Statutory Guidelines made under the PPIP and HRIP Acts

Other relevant legislation

- *Crimes Act 1900 (NSW)*
- *Government Information (Public Access) Act 2009 (NSW)* (GIPA Act)
- *State Records Act 1998*
- *Workplace Surveillance Act 2005*

Privacy Management Plan

PART F: Policies affecting processing of personal and health information

The Service NSW Privacy team helps Service NSW staff understand their obligations when dealing with personal information. How we collect and what we do with personal information is critical to building trust with our customers in Service NSW and the government.

The Privacy team has developed a range of guidance material to help staff understand how privacy operates in Service NSW, and how staff can protect the information Service NSW handles. This information can be accessed via the Service NSW intranet.

There are a range of other Service NSW policies and procedures that are related to the handling of personal information that staff can access via the Service NSW Intranet. These include:

- Service NSW *Code of Conduct*. Section “Using and protecting confidential information” and Section “Responsibilities, accountabilities and expectations” relate to confidentiality, the security of information, and compliance with privacy obligations
- Service NSW *Internet and Email Usage Policy*
- Service NSW *Media and Social Media Policy*
- Service NSW *Information Security Policy*

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 we hold about you, for example, if you need to update your contact details.

Service NSW must provide access to or amend personal or health information without excessive delay and without expense. We do not charge any fees to access or to amend personal or health information unless you are lodging a formal application under the GIPA Act (see below).

Informal and formal requests

Informal requests

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

You are encouraged to contact the relevant business unit with Service NSW directly if you are trying to access or amend your information. You can also contact the Service NSW Privacy Officer.

In many cases, Service NSW will be able to amend your personal or health information on the spot, but we 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. You would generally need to complete a particular form and provide specific details before your application will be valid. You can find out about making formal access applications under GIPA via our website at https://www.service.nsw.gov.au/accessing-information.

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.

Formal requests for your personal or health information (whether you are a member of the public or a staff member) should be sent to the Service NSW 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

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* 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 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 whether personal information will be revealed, as well as any breach of the IPPs and HPPs, as public interest considerations against disclosure.

Privacy Management Plan

PART H: Privacy complaints

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 first to discuss any concerns with the staff member or business unit dealing with your information (if known).

Any person may make a complaint:

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

General privacy complaints

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

There are no external review rights to NCAT at the conclusion of a general privacy complaint.

If a customer is not satisfied with the outcome of their 'general complaint' then they may still apply for a privacy internal review. By law, a customer has 6 months from first becoming aware of the relevant conduct to apply for an internal review. Service NSW may decline to deal with an application for internal review received after that period.

Internal Review

Internal review is the process by which Service NSW manages formal, written privacy complaints about how we have dealt with personal information. You can request an internal review by contacting the Service NSW Privacy Officer, by phone on 13 77 88 or by email at privacy@service.nsw.gov.au. Service NSW conducts its own internal reviews, and no longer discloses information about these to the Department of Customer Service.

We consider all written complaints we receive about Service NSW's handling of your personal or

health information to be a possible application for a privacy internal review, even if the applicant doesn't use the words 'internal review' or specifically refer to the privacy legislation. However, to constitute an application for internal review, the written complaint must, on its face, reasonably convey to Service NSW that an application for internal review is sought.

The absence of any reference to privacy legislation, information protection principles or the concept of privacy may indicate to Service NSW that a complaint is an expression of grievance and request for action rather than an application for internal review. Wherever possible, Service NSW will attempt to clarify with customers their intentions in submitting a complaint in order to establish the customer's preferred pathway – a general complaint or an internal privacy review or another outcome – where a customer's intentions are not evident in their complaint.

Under privacy law, an internal review must be undertaken by the agency concerned. This means that, if you apply to Service NSW for an internal review of its conduct, Service NSW must undertake the review.

Where an application for internal review relates to conduct by Service NSW exercising functions in its own right, Service NSW will not conduct inquiries with any other agency without first seeking the applicant's consent.

Where an application for internal review relates to conduct by Service NSW exercising functions for a partner agency, Service NSW may conduct inquiries with the relevant partner agency in order to make findings and determine what action, if any, to take.

Service NSW is allowing applications for internal review to be received up to 12 months following the date of letters notifying customers that they are impacted by the 2020 cyber-attack and associated data breach.

In other cases, Service NSW will consider requests for late applications for internal review on a case by case basis and may agree to a late application where a customer experiences hardship or another barrier preventing them from lodging an application within six months.

Requirements

Under the privacy laws, an application for internal review must:

- be in writing

- be addressed to Service NSW
- specify an address in Australia to which the applicant is to be notified after the completion of the review, and
- be lodged at Service NSW 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.

The IPC website provides a form for applying for internal review, as an optional resource. This can be downloaded from their website at www.ipc.nsw.gov.au. Although we encourage you to use the form, it is not compulsory. You may submit any other relevant material along with your application.

What you can expect from us

- Your application will be acknowledged in writing and the acknowledgement will include an expected completion date.
- We will determine whether the internal review should be handled by Service NSW alone or in consultation with any relevant partner agency.
- The internal review will be conducted by the Service NSW Privacy Officer, or by another person who:
    - was not involved in the conduct which is the subject of the complaint; and
    - is an employee or an officer of Service NSW, and
    - is qualified to deal with the subject matter of the complaint.
- 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).
- 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 Service NSW as part of the internal review process.
- In making a decision, we 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, 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 Service NSW 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 internal 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 decisions.

External Review by the NSW Civil & Administrative Tribunal (NCAT)

People may apply to NCAT for an external review of the conduct which was the subject of their earlier internal review application. NCAT may make orders requiring Service NSW 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 Service NSW to pay damages if the applicant has suffered financial loss or psychological or physical harm as a result of the conduct.

Privacy Management Plan

PART I: Strategies for implementing and reviewing this Plan

Communicating this Plan

Public Awareness

The plan is a commitment of service to our customers and stakeholders of how we manage personal information and health information. It is central to how we do business.

We will publish this plan on our website in a format that is accessible to the widest possible audience, regardless of technology or ability.

Service NSW 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*;
- using the plan as part of induction for new employees, agents, and contractors;
- Using the plan as an everyday reference point for our privacy management practice.

Service NSW employees and contractors

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 through mandatory, privacy specific training for all employees and contractors
- 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
- providing refresher training 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 during Privacy Awareness Week and at other times during the year.

Reviewing this Plan

Service NSW's first PMP was drafted in early 2013 and has been reviewed since. This edition is a review undertaken in March 2022. Service NSW will review this PMP regularly, and update it as required

If you have any feedback on this document please contact the Service NSW Privacy Officer: by mail at GPO Box 7057 Sydney NSW 2001, by phone to 13 77 88, or by email to privacy@service.nsw.gov.au.

Privacy Management Plan

PART J: Contacts

Service NSW Privacy Officer

Phone:	13 77 88
Email:	privacy@service.nsw.gov.au
Website:	www.service.nsw.gov.au/privacy
Mail:	Service NSW Privacy Officer Risk, Strategy and Performance Division GPO Box 7057 Sydney NSW 2001
Office:	McKell Building, 2-24 Rawson Place, Haymarket NSW 2000

The Information and Privacy Commission NSW

Phone:	(02) 9619 8672
Email:	ipcinfo@ipc.nsw.gov.au
Website:	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

Phone:	1300 006 228 and select Option 3 for all Administrative and Equal Opportunity Division enquiries
Email:	aeod@ncat.nsw.gov.au
Website:	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 we handle personal and health information.

Government Information (Public Access) Act 2009 **(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 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, please contact DCS's GIPA team at gipa@customerservice.nsw.gov.au or on (02) 9219 3700.

General Data Protection Regulation (GDPR)

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

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.

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 (NSW) 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 2: Exemptions

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

Limiting our 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 we collect 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 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 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

- where another law authorises or requires us not to comply
- where non-compliance is otherwise permitted, implied, or contemplated by another law.

Access – IPP 7 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 and HPP 8

- health information collected before 1 September 2004
- 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
- the provisions of 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
- 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 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.

Appendix 3: Guide to drafting Privacy Notices

Service NSW is responsible for providing a privacy notice for every customer transaction.

Where Service NSW collects personal information in its own right, including for its own internal administrative purposes, it must make customers aware of the specified matters.

Where Service NSW exercises customer service functions on behalf of a partner agency, it will either provide the customer with a privacy notice supplied or endorsed by the partner agency (e.g. on partner agency paper or online forms, or in relevant telephone scripts), or will refer the person to information provided by a partner agency in relation to the collection of the information.

The following principles guide the drafting of privacy notices for customer service transactions:

- the Service NSW Privacy Officer must approve the wording and location of all privacy notices; the partner agency must approve the wording of the privacy notice
- if the transaction can occur across more than one service channel, the privacy notice should be worded as closely as possible across each channel
- however, there will need to be some differences for the Contact Centre channel. For example, in the Digital or Service Centre channels, a mandatory field is easily denoted by an asterisk on the online or paper form. While the design of a Salesforce data entry field may also allow for this, the script for Contact Centre operators may need additional verbal explanation for the customer
- wording should be concise and in plain language
- the notice should clarify what Service NSW will do with the information, as well as what the partner agency will do with the information
- the notice should be given / visible before any data collection begins
- in the Service Centre channel, notice can be provided on the paper forms developed and supplied by the partner agency
- in the Digital channel, the notice should be given on the landing page for that transaction, even if it also appears later in the process, and
- in the Digital channel, if the data is being collected and stored by Service NSW (such as for the Seniors Card database), the notice should also appear on the first data collection page.

At the end of each privacy notice should be added:

Privacy Management Plan

Read the Service NSW privacy statement for more information on how:

- we handle your personal information
- you can access and seek correction of the information
- privacy enquiries or complaints can be made.

You can call Service NSW on 13 77 88.

Service NSW is located at 2-24 Rawson Place Sydney NSW 2000.

Appendix 4: List of Partner Agencies, Agreements and Organisations

Australian Government

- Regional Development Australia NSW
- Services Australia

NSW Government

- **Customer Service Cluster:** NSW Registry of Births, Deaths and Marriages, NSW Fair Trading, Liquor and Gaming, Revenue NSW, Subsidence Advisory NSW, State Insurance Regulatory Authority, SafeWork NSW
- **Education Cluster:** Department of Education, Training Services NSW, Study NSW
- **Health Cluster:** Ministry of Health, Health Pathology, eHealth NSW **Planning, Industry and Environment Cluster:** Energy Consumers and Programs, Public Works Advisory, BASIX, Water, Environment Protection Authority, National Parks and Wildlife Services, Office of Local Government, Housing and Property, Planning and Assessment
- **Premier and Cabinet Cluster:** Resilience NSW, Create NSW, Department of Premier and Cabinet
- **Regional NSW Cluster:** NSW Rural Assistance Authority, Local Land Services, Department of Regional NSW
- **Stronger Communities Cluster:** NSW Civil and Administrative Tribunal, Office of Veterans Affairs NSW, NSW Trustee and Guardian, NSW Corrective Services, NSW Police, Department of Communities and Justice, Multicultural NSW, Office of the Children's Guardian, Office of Sport, Housing NSW, DCJ Seniors.
- **Transport Cluster:** NSW Trainlink. Roads and Maritime Services, Opal, Point to Point Authority, Port Authority, Toll Relief, e-Toll, (National Heavy Vehicle Register)
- **Treasury Cluster:** NSW Procurement, Small Business Commissioner, NSW Treasury,
    - **State Owned Corporations:** Hunter Water
    - **Public Financial Corporations:** iCare

NSW Local Government

- Council of the City of Parramatta
- Byron Shire Council

- Newcastle City Council
- Queanbeyan-Palerang Regional Council

Organisations other than government

- Carers NSW
- NRMA