The SSI Way for...
Legal & Compliance

Settlement Services International

Privacy Management Plan

Version 1.1, January 2019

Table of Contents

1 OVERVIEW

1.1 Purpose

This Privacy Management Plan (**Plan**) has the following purposes, being to:

- meet the requirement to have such a plan under section 33 of the *Privacy and Personal Information Protection Act 1998* (NSW) (**PPIPA**);
- demonstrate to members of the public how we meet our obligations under PPIPA and the *Health Records and Information Privacy Act 2002* (NSW) (**HRIPA**);
- provide staff with the necessary knowledge and skills to manage personal and health information appropriately and in accordance with the law;
- enhance the transparency of our operations, and
- illustrate our commitment to respecting the privacy rights of our customers, clients, staff and members of the public.

1.2 Scope

This plan applies to Settlement Services International's (SSI's) treatment of all personal and health information, whether it relates to a customer or client, an employee or another person (such as a contractor).

1.3 Introduction

SSI collects, holds, uses and discloses personal and health information for the purpose of carrying out our functions. We take privacy seriously and will protect personal and health information pursuant to PPIPA and HRIPA with reference to this plan.

PPIPA and HRIPA set out baseline privacy standards or 'privacy principles' which SSI must comply with. PPIPA covers personal information other than health information, and requires SSI to comply with 12 Information Protection Principles (IPPs). The IPPs cover the complete information life cycle from collection through to disposal. The IPPs include obligations with respect to data security, data quality and rights of access and amendment to one's own personal information, as well as how personal information may be collected, used and disclosed.

Health information is regulated by a similar yet separate set of principles set out in HRIPA. While health information is excluded from the definition of 'personal information' in PPIPA, it is viewed as a type of personal information that relates to information about the physical or mental health of an individual or information provided or generated in the delivery of a health service. There are 15 Health Privacy Principles (HPPs) with which SSI must comply. Like the IPPs, the HPPs cover the entire information life cycle, but also include some additional principles with respect to anonymity, trans-border data flows, linkage of health records and the use of unique identifiers.

There are exemptions to many of the privacy principles and public register provisions. Exemptions can be found in PPIPA and HRIPA, and in regulations, privacy codes of practice and public interest directions.

At SSI, privacy matters are managed by the Legal & Compliance team.

1.4 Responsibilities of staff

SSI will ensure that its staff are aware of their privacy responsibilities and are complying with SSI's privacy policies, procedures, guidelines and standards, including this plan.

All SSI staff are required to comply with PPIPA and HRIPA, including the IPPs and HPPs when handling personal and health information held by the organisation. Both Acts contain criminal offence provisions applicable to persons who misuse personal and health information.

This plan aims to assist SSI staff to understand and comply with their obligations under both PPIPA and HRIPA.

SSI staff should identify whether any of their new projects or programs are likely to raise any privacy issues. The NSW Privacy Commissioner has developed a checklist available at https://www.ipc.nsw.gov.au/checklist-identifying-privacy-issues to assist staff identify when there may be privacy issues early in a project's design stage. Please utilise the checklist and contact the Legal & Compliance team if need be.

2 PERSONAL & HEALTH INFORMATION

2.1 What is personal information?

Personal information is defined in section 4 of PPIPA. In summary, personal information is information or an opinion about an individual whose identity is apparent or can be reasonably ascertained from the information or opinion. It is not restricted to information that clearly identifies a person but may include information which leads to the identification of an individual when considered in association with other available information. Personal information can include a record which may contain your name, address and other details about you, your, bank account details, fingerprints, or a photograph or video. It can also include information that is recorded (for example, on paper or contained in a database) and also information that is not recorded (for example verbal conversations).

2.2 What does not constitute personal information?

Exclusions as to what constitutes personal information can be found at sections 4(3) and 4A of PPIPA. There are 13 exclusions to the definition of personal information under PPIPA, including:

- information about an individual who has been dead for more than 30 years;
- information about an individual that is contained in a publicly available publication, and
- information or an opinion about an individual's suitability for appointment or employment as a public sector official.

Common examples of information falling within the exclusions include recruitment records, referee reports and performance appraisals, as well as information provided in the White Pages, a newspaper or a court judgment available on the internet. PPIPA also excludes from its sphere of operation certain information which may be held in connection with a number of activities authorised under a variety of legislation. For more information on these exclusions reference should be made to sections 4(3) and 4A of PPIPA or contact made with the Legal & Compliance team.

2.3 What is health information?

Health information is defined in section 6 of HRIPA. Health information means:

- personal information that is also information or an opinion about:
    - a person's physical or mental health or disability;
    - a health service provided, or to be provided, to a person;
    - a person's express wishes about the future provision of health;
- other personal information collected to provide a health service;
- other personal information about an individual collected in connection with the donation of an individual's body parts, organs or body substances; or
- genetic information that is or could be predictive of the health of a person or their relatives or descendants.

Exclusions as to what constitutes health information pursuant to HRIPA can be found at section 5(3) of HRIPA. There are 15 exclusions to the definition of health information under HRIPA.

HRIPA also excludes from its sphere of operation certain information which may be held in connection with a number of activities authorised under a variety of legislation.

2.4 Main kinds of personal and health information held by SSI

SSI collects and holds personal information and health information in order to provide efficient services to both staff and clients.

Personal information

Personal information collected by SSI about employees and contractors may include, but is not limited to:

- payroll information (e.g. salary details, bank account details)
- personnel files
- information held on the HR Information System database (e.g. address, salary details, birth date)
- leave applications
- investigation files (safety, grievance, fraud and/or corrupt conduct)
- accident/incident records and witness statements
- performance management and feedback records
- training records
- job applications
- images of individuals for use on staff security cards
- declared conflicts of interest.

Personal information collected by SSI about clients may include, but is not limited to:

- address and telephone numbers
- banking details
- details about other family members
- orientation training records
- needs assessment (including accommodation requirements)
- assessment of suitability of accommodation to be provided by friends or family.

We may also collect:

- information about individuals obtained in the course of developing and managing business relationships and maintaining contractual relationships, and
- information obtained in the course of complaint handling.

Health information

Health information collected by SSI about employees and contractors may include, but is not limited to:

- sick leave information such as leave applications and medical certificates
- workers compensation files and claim forms
- employee disclosures of pre-existing medical conditions.

Health information collected by SSI about clients may include, but is not limited to:

- pre-arrival and post-arrival health assessments
- referrals to health services.

2.5 Confidentiality of records

Employees, contractors or volunteers who collect, or have access to personal information or health information to enable them to perform their duties with SSI must not access this information inappropriately nor disclose information without authorisation.

Managers/supervisors are responsible for ensuring that personal and health information retained in their area/program is managed in accordance with this plan.

Employees, contractors or volunteers who unintentionally receive access to personal or health information must maintain confidentiality of that information and must notify their direct manager that they received access to that information. Managers must ensure, where practicable, work processes are modified to prevent unintentional access being repeated.

3 APPLYING THE PRIVACY PRINCIPLES

3.1 Collection

IPP 1 / HPP 1 – Lawful

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

SSI will only collect personal and health information if:

- it is for a lawful purpose that is directly related to one of SSI's functions or activities, and
- it is reasonably necessary for SSI to collect the information for that purpose.

IPP 2 / HPP 3 – Direct

IPP2 – An agency must only collect personal information directly from the individual, unless the individual has authorised collection from someone else, or if the information relates to a person under age of 16, it has been provided by a parent or guardian.

HPP3 – An organisation must collect health information about an individual only from that individual, unless it is unreasonable or impracticable to do so.

Wherever possible, SSI will collect personal and health information directly from the individual the information relates to unless:

- the individual is under 16 years of age, in which case SSI may instead collect personal information from the parent or guardian
- the individual has authorised collection of the information from someone else, in which case SSI may collect the information from that nominated person, and
- it would be unreasonable or impracticable to collect health information from the individual, in which case we may collect health information from another source. The NSW Privacy Commissioner's Handbook to Health Privacy provides some examples of when it might be unreasonable or impractical to collect health information directly from the person. Health information should be collected in accordance with these guidelines.

This principle is designed to limit the collection of your personal information without an individual's knowledge. Secret or undisclosed collections may prevent an individual from exercising their rights.

IPP 3 / HPP 4 – Open

Before or as soon as practicable after collection, an agency must inform an individual that the information is being collected, why it is being collected, who will receive it, how it will be used, and to whom it may be disclosed. Individuals must also be told how they can access and correct their personal and health information, if the information is required by law or is voluntary, and any consequences that may apply if they decide not to provide it.

SSI will take reasonable steps to ensure that the person whose information is being collected is aware of the fact of collection. SSI will inform individuals of the following:

- the fact that the information is being collected
- the reason the information is being collected
- the parties to whom the information is usually disclosed to
- how the individual can access and correct the information being collected, and
- the consequences that may apply if the individual decides not to provide that information.

SSI informs individuals of the above matters through its privacy statements and consent forms as required. Consent is a key control to ensure the individual has understood and provided informed consent. Where the supply of information is voluntary (i.e. it is not required by law), SSI will explain the consequences of not supplying it.

IPP 4 / HPP 2– Relevant

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

When collecting information, SSI will:

- not collect excessive personal or health information
- not collect personal or health information in an unreasonably intrusive manner, and
- ensure that personal and health information collected is relevant, accurate, up-to-date and complete.

Business units and programs that collect information will implement procedures to ensure the information they hold is kept up to date and relevant. SSI mostly collects information through the use of forms which only contain relevant fields to ensure the organisation is not collecting excessive information.

3.2 Storage

IPP 5 / HPP 5 – Secure

An agency must store personal information securely, keep it no longer than necessary and dispose of it appropriately. It should also take reasonable security safeguards to protect personal information from unauthorised access, use, modification or disclosure.

The security of personal information collected by SSI is paramount, whether this information is in computer or online systems, or in paper-based form. This means that personal information must be protected from unauthorised access, alteration, use and disclosure.

SSI will ensure that personal and health information is stored securely, not kept longer than necessary, and is disposed of appropriately. Where it is necessary for personal or health information to be transferred to a person in connection with the provision of a service, SSI will take steps to prevent unauthorised use and disclosure of that information.

Digital Information Security

SSI's IT systems are designed to ensure that only authorised users can access them. Access controls are also utilised to restrict access to information based on the user's particular role and function.

The use of strong passwords by staff is enforced when using work computers, portable devices and email communications. Security software has been deployed across all network components, including the servers and network gateways. Security considerations are also taken into account in arrangements for data transmission, backup and storage.

Further, SSI also has comprehensive policies, procedures and processes in place to appropriately respond to any instance of unauthorised access to, use of or disclosure of personal and health information.

All SSI employees are responsible for identifying and reporting events or issues with possible information security implications as quickly as possible. Prompt reporting enables prompt assessment, timely investigation and corrective action to be taken if necessary. This also applies to security or data breaches.

Records management

Physical security is an important part of ensuring information is not inappropriately accessed. Our staff have access to secure storage spaces near their workstations to secure documents and devices which may contain personal or health information.

SSI keeps information for only as long as necessary or as required by law, reducing the risk that it may be mishandled. If the organisation finds it has no further need for personal information, it may be archived in accordance with SSI's record retention obligations or securely destroyed in a secure manner as appropriate (for example, using secure, locked recycling bins and shredders).

3.3 Access and accuracy

IPP 6 / HPP 6 – Transparent

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

SSI will take reasonable steps to ensure the information it holds and uses is relevant, accurate, up to date, and not misleading, having regard for the purposes for which it was collected and any purpose(s) directly related to that purpose (this is considered the primary purpose of collection).

Individuals have a right to know:

- whether information about them is held by SSI
- the nature of the information being held
- the main purpose(s) for which it is being used
- how they can access their information (and ensure valid requests for access proceed without excessive delay or expense)
- how they can correct this information it if it is not accurate.

If an individual wishes to know whether SSI holds personal or health information, they should contact the organisation's Privacy Officer (feedback@ssi.org.au, (02) 8799-6700). If the organisation does hold personal or health information, SSI's Privacy Officer can advise an individual of the nature of that information, the main purposes for which the information is used, and the individual's right of access to that information.

IPP 7 / HPP 7 – Accessible

An agency must allow access to personal and health information without excessive delay or expense.

SSI will allow people to access their personal and health information without excessive delay or expense. SSI will only refuse access where authorised by law, and will provide written reasons, if requested.

Providing an individual access to their own information gives them the opportunity to find out what information SSI holds about them. SSI will let any individual see their own personal and health information in accordance with PPIPA and HRIPA, in many cases at no cost and through an informal request process. Applications for access will be processed in a timely fashion.

The Information & Privacy Commission's Best Practice Guide Privacy and People with Decision-making Disabilities explains how to provide access to information held about a person who has limited or no capacity.

IPP 8 / HPP 8 – Correct

An agency must allow an individual to update, correct or amend personal and health information where necessary.

Providing individuals with access to, and correction of, their information ensures individuals have control over their information by providing an opportunity to correct inaccurate, irrelevant and out-of-date information. SSI actively encourages individuals to help keep any information the organisation holds up-to-date, complete and accurate by contacting SSI with updated information.

Once a request has been made to amend information, SSI will make appropriate amendments – whether by way of corrections, deletions or additions. When amending the information, SSI will have regard to the purpose for which the information was collected.

Where practicable, SSI will also notify recipients of any amendments. SSI will consider the following factors when determining what is practicable:

- who the recipients of the information are
- the purpose for which the information was collected
- the sensitivity of the information
- the number of people who will have access to the information
- the importance of accuracy of the information
- the potential effects to the individual concerned if the information is inaccurate, out-of- date or irrelevant
- the ease of notifying recipients, and
- the costs of notifying recipients.

Requests for changes to personnel records will be processed by PAC and in accordance with relevant policies.

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

3.4 Use

IPP 9 / HPP 9 – Accurate

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

SSI must take reasonable steps to ensure that the information it holds is relevant, accurate, up to date, and not misleading, having regard to the purpose(s) for which the information is to be used.

SSI will not use personal or health information where it is known to contain erroneous information.

What might be considered 'reasonable steps' will depend upon the circumstances, but some factors to take into account are:

- the context in which the information was obtained
- the purpose for which the information was collected
- the purpose for which the information will now be used
- 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 already given to the person to correct inaccuracies, and

- the effort and cost involved in checking the information.

IPP 10 / HPP 10 – Limited

The use of personal and health information held by the agency is limited to the primary purpose(s) for which it was collected, unless an exemption applies.

SSI may use personal and health information for:

- the primary purpose for which it was collected
- a directly related secondary purpose
- another purpose where it is reasonably necessary to prevent or lessen a serious and imminent threat to life or health, or
- another purpose for which the individual has consented.

A directly related secondary purpose is a purpose that is very closely related to the purpose for collection and would be the type of purpose that people would quite reasonably expect their information to be used for.

Examples of uses that are directly related to each other include quality assurance activities such as monitoring, evaluating and auditing.

SSI will take reasonable steps to ensure that personal and health information is accessible only by those staff members who need to access it in order to carry out their duties.

Further to the circumstances set out above, SSI may also use health information to lessen or prevent a serious threat to public health or safety, finding a missing person, for law enforcement purposes and in respect of suspected unlawful activity, unsatisfactory professional conduct or breach of discipline.

The NSW Privacy Commissioner's Best Practice Guide 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.

3.5 Disclosure

IPP 11 – Restricted / HPP 11 - Limited

An agency can only disclose personal and health information for secondary purposes in limited circumstances as set out in the Privacy Acts.

Under the PPIPA, SSI can disclose personal information for a secondary purpose if:

- the individual consented, or
- the secondary purpose is directly related to the primary purpose and SSI reasonably believed the individual would not object to the disclosure, or
- SSI reasonably believes on reasonable grounds the disclosure is necessary to prevent a serious and imminent threat to any person's life, health or safety.

In addition to the above, SSI cannot disclose an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities ("**personal sensitive information**") unless the disclosure is necessary to prevent a serious or imminent threat to the life or health of any individual.

Under the HRIPA, SSI can disclose an individuals' health information for a secondary purpose if:

- the individual has consented, or
- the secondary purpose is directly related to the primary purpose for which the information was

collected, and the individual would reasonably expect SSI to disclose that information for a secondary purpose, or
- where an individual has been made aware, or is likely to be aware, that information of that kind is usually disclosed to the body or person that SSI wishes to disclose the information to, or
- SSI believes, on reasonable grounds, that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life, health or safety of a person or a serious threat to public health or safety, or
- SSI has reasonable grounds to suspect an unlawful activity has been or may be engaged in, or
- necessary for the exercise of law enforcement functions by law enforcement agencies, or
- necessary for the exercise of complaint handling functions or investigative functions by investigative agencies, or
- the disclosure is permitted by a Public Interest Direction made by the NSW Privacy Commissioner.

In some instances, SSI may be required to release information to third parties by law. For example, SSI may be required by law to release information to Commonwealth government agencies such as the Department of Education, Employment and Workplace Relations (DEEWR) and the Department of Immigration and Border Protection (DIBP) if requested under a relevant section of legislation that governs the Departments.

SSI also has discretion to, and can be required to, release information to law enforcement agencies in relation to law enforcement, for example:

- in relation to proceedings for an offence including in response to a subpoena or search warrant
- to a law enforcement agency in relation to a person reported as missing
- if reasonably necessary for the protection of public revenue or to investigate an offence where there are reasonable grounds to believe that an offence has been committed.

Trans-border disclosure of personal information

SSI will not disclose personal information to any person or body in a jurisdiction outside NSW or to a Commonwealth agency unless:

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

Before making a trans-border disclosure, SSI will make the assessment required by section 19(2)(a) and HPP 14. These require a disclosing agency to be satisfied that the privacy protections substantially similar to those in NSW operate in the destination jurisdiction.

Trans-border disclosure of health information

SSI can only transfer health information outside NSW if one of the following applies:

- the individual concerned has consented
- if it is necessary for a contract with (or in the interests of) the person concerned
- if it will benefit the person concerned and it is impracticable to 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
- SSI have bound the recipient by contract to privacy obligations equivalent to the HPPs, or
- if it is permitted or required by legislation or any other law.

We can, however, disclose health information (whether within or outside NSW) to prevent a serious and imminent threat to life, health or safety of an individual or a serious threat to public health or safety.

IPP 12 – Safeguarded

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

There are stricter obligations for the disclosure of personal sensitive information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, health, and sexual activities. SSI will not disclose this information unless it is reasonably necessary for law enforcement purposes, is required by law or if the disclosure is necessary to prevent a serious or imminent threat to the life or health of a person.

The same restrictions on trans-border disclosures apply to this type of information.

3.6 Identifiers

HPP 12 – Not identified

An agency must only identify people by using unique identifiers if it is reasonably necessary to carry out the agency's functions efficiently.

An identifier is defined in section 4 of the HRIPA to mean something that an organisation assigns to a person in order to uniquely identify that person (usually a number). The identifier will have either been created, adopted, used or disclosed in conjunction with or in relation to the person's health information. A person's name is not an identifier.

SSI will ensure that unique identifiers are only assigned to individuals in relation to their health information if it is reasonably necessary for the organisation to carry out its functions efficiently.

An identifier does not need to use a person's name as they are designed to be unique to a specific individual (for e.g. a customer number, unique patient number, tax file number or driver's license number). Identifiers will be perceived as health information and subject to HRIPA.

3.7 Transferrals and linkage

HPP 14 – Controlled

In addition to the normal disclosure rules under HPP11 of HRIPA, the same disclosure restrictions (Trans-border flows and Commonwealth agencies) apply to health information (see section 3.5 above).

HPP 15 – Authorised

An agency must not include health information or disclose an individual's identifier for inclusion in health information in a health records linkage system unless the individual has provided their express consent.

SSI will only use health records linkage systems when individuals have expressly consented to their information being included on such a system.

Exemptions

PPIPA and HRIPA provide that an agency need not comply with some or all of the IPPs or HPPs if certain circumstances apply.

Some examples of exemptions include:

- unsolicited information
- use or disclosure for law enforcement purposes or investigative functions
- where another law authorises or requires the organisation not to comply
- where non-compliance is lawfully authorised or required
- where compliance would prejudice the individual
- when the organisation exchanges information with other public sector agencies.

If an exemption applies to a particular situation, SSI will inform the individual(s) concerned about the exemption and why it applies, as is reasonable and appropriate in the circumstances.

4 COMPLAINTS AND BREACHES

4.1 Complaints

SSI is committed to protecting the privacy of personal and health information of staff, contractors, volunteers and clients in accordance with the privacy legislation.

To make a complaint

If you think your privacy has been breached, you can make a complaint in one of the following ways:

- Contact the program or division involved and resolve the matter informally
- Follow SSI's complaints procedure by sending an email to feedback@ssi.org.au or downloading the Compliments and Complaints form from on our website (https://www.ssi.org.au/contact-us)
- Contact the Privacy Officer at feedback@ssi.org.au to request an internal review
- Contact the Privacy Commissioner:
    - Office: Level 17, 201 Elizabeth Street, Sydney 2000
    - Postal address: GPO Box 7011, Sydney NSW 2001
    - Email: ipcinfo@ipc.nsw.gov.au
    - Tel: 1800-472-679

4.2 Internal reviews

If an individual does not feel the complaints procedure has resolved their issue regarding the use or misuse their personal or health information, they can lodge a written request to the Privacy Officer (feedback@ssi.org.au) for an internal review.

SSI will conduct an internal review to determine:

- whether or not the alleged conduct occurred,
- if so, whether the organisation has complied with its privacy obligations,
- if not, whether non-compliance was authorised by an exemption, Privacy Codes of Practice, a direction from the Privacy Commissioner or an appropriate action by way of a response/remedy.

If the complaint is about an alleged breach of the IPPs, HPPs, privacy code of practice or health privacy code of practice, the internal review will be conducted by a person who:

- was not involved in the conduct which is the subject of the complaint
- is an employee or an officer of the agency, and
- is qualified to deal with the subject matter of the complaint.

Internal reviews will be completed within 60 days of the receipt of a formal application for review. Once the internal review is completed, SSI will advise the individual and the NSW Privacy Commissioner of its findings and what it will do as a result.

The role of the NSW Privacy Commissioner in internal reviews

The NSW Privacy Commissioner has an oversight role in the internal review process and may make submissions on internal reviews.

SSI is required under the Privacy legislation to notify the NSW Privacy Commissioner regarding the following:

- formal complaints received
- progress on internal reviews being undertaken, and
- findings of the reviews undertaken and the action proposed to be taken by SSI.

The Privacy Commissioner is entitled to make submissions to SSI with respect to the findings of the internal review and may at the request of SSI undertake the internal review on behalf of SSI.

4.3 Lodging a complaint with the Privacy Commissioner

A person aggrieved by the conduct of SSI may complain directly to the NSW Privacy Commissioner, not as an external review mechanism, but as a complaint.

In this instance, the Privacy Commissioner may conduct a preliminary assessment of a complaint before deciding whether to deal with the complaint.

The Privacy Commissioner must inform the complainant of the internal review process available under Part 5 of PPIPA and may decide not to deal with the complaint if satisfied that:

a) the complaint is frivolous, vexatious or lacking in substance or not in good faith, or
b) the subject matter of the complaint is trivial, or
c) the subject matter of the complaint relates to a matter permitted or required by or under any law, or
d) there is available to the complainant an alternative, satisfactory and readily means of redress, or
e) it would be more appropriate for the complainant to make an application for an internal review under section 53.

If the Privacy Commissioner does decide to deal with the complaint, it must endeavour to resolve the complaint by conciliation.

The Privacy Commissioner may refer a complaint made to it to another person or body for investigation or other action, if considered appropriate.

When the NSW Privacy Commissioner deals with the complaints against SSI, the Privacy Commissioner does not have determinative powers (i.e. the Privacy Commissioner cannot set aside or vary the decision of the organisation or award compensation).

The Privacy Commissioner can be contacted as follows:

- Office: Level 17, 201 Elizabeth Street, Sydney 2000
- Postal address: GPO Box 7011, Sydney NSW 2001
- Email: ipcinfo@ipc.nsw.gov.au
- Tel: 1800-472-679

5 OFFENCES

Part 8 of the PPIPA and HRIPA details offences for certain conduct. A table detailing the relevant penalties and associated provision has been provided below.

Offence	Maximum penalty	Legislative provision
It is a criminal offence for a public sector official to corruptly disclose and use personal or health information.	Fine of up to 100 penalty units ($11,000) or imprisonment for two years, or both.	s 62 of PPIPA and s 68 of HRIPA
It is a criminal offence for a person to offer to supply personal or health information that has been disclosed unlawfully.	Fine of up to 100 penalty units ($11,000), or imprisonment for two years, or both	S 63 of PPIPA and s6 9 of HRIPA
It is a criminal offence for a person – by threat, intimidation or misrepresentation – to persuade or attempt to persuade an individual: • to refrain from making or pursuing a request to access health information, a complaint to the Privacy Commissioner or the NSW Civil and Administrative Tribunal, or an application for an internal review; or • to withdraw such a request, complaint or application.	Fine of up to 100 penalty units ($11,000).	s 70(1) of HRIPA
A person must not – by threat, intimidation or misrepresentation – require another person to give consent under HRIPA, or require a person to do, without consent, an act for which consent is required.	Fine of up to 100 penalty units ($11,000).	s 70(2) of HRIPA
It is a criminal offence for a person to: • wilfully obstruct, hinder or resist the Privacy Commissioner or a member of the staff of the Privacy Commissioner • refuse or wilfully fail to comply with any lawful requirement of the Privacy Commissioner or a member of the staff of the Privacy Commissioner, or • wilfully make any false statement to or mislead, or attempt to mislead, the Privacy Commissioner or a member of the staff of the Privacy Commissioner • in the exercise of their functions under PPIPA or any other Act.	Fine of up to 10 penalty units ($1100).	s 68(1) of PPIPA.

6 PROMOTING PRIVACY

6.1 Staff training and education

SSI provides training and education seminars to staff to inform them of their responsibilities under the Privacy Acts. Privacy news and updates are communicated to all staff on a regular basis.

Policies and procedures which may impact the management of personal or health information are communicated to staff in a range of ways, including through the organisation's intranet (SSI Central) and training. The Code of Conduct specifically refers to the importance of protecting privacy and complying with relevant legislation.

The Privacy Officer (with advice from a solicitor as appropriate) will also provide tailored advice to SSI staff to support them in understanding and meeting their privacy obligations. For example, the Privacy Officer can provide advice about:

- whether personal or health information is being collected, used or disclosed for a lawful purpose
- if that lawful purpose is directly related to a function of the organisation or a secondary purpose
- whether or not the collection of that personal information is reasonably necessary for the specified purpose
- whether any exemptions apply
- how to make a complaint or request an internal review
- the internal review process.

6.2 Public awareness

SSI promotes public awareness of the privacy obligations by:

- the publication of this plan on the SSI website
- maintaining a dedicated privacy page on the SSI website for all privacy resources and contacts, including the organisation's privacy policy
- providing a dedicated Privacy Officer to manage privacy related issues, complaints and investigations
- making staff, contractors, volunteers, clients and members of the public aware of the privacy obligations when completing forms that collect personal and health information.

Where the public has additional questions, they are encouraged to contact the Privacy Officer at feedback@ssi.org.au or the Privacy Commissioner as below:

Office: Level 17, 201 Elizabeth Street, Sydney 2000
Postal address: GPO Box 7011, Sydney NSW 2001
Email: ipcinfo@ipc.nsw.gov.au
Tel: 1800 472 679

7 DOCUMENT CONTROL

7.1 Related Documents

Related Policies/Procedures	
CPAC.PO.01	Code of Conduct Policy
CLC.PO.07	Privacy Policy
CLC.PR.11	Data Protection Procedure
CIT.PO.01	Information Technology & Communications Policy

References	
https://www.ipc.nsw.gov.au/checklist-identifying-privacy-issues	Checklist - Identifying privacy issues, Information and Privacy Commission
https://www.ipc.nsw.gov.au/sites/default/files/file_manager/hripa_health_handbook.pdf	Handbook to health privacy, Privacy NSW
http://ipc.nsw.gov.au/sites/default/files/file_manager/bpg_disability_2004.pdf	Privacy and people with decision-making disabilities, Privacy NSW

7.2 Document History

Version	Created	Author	Description
1	November 2017	P&P Project Manager	Approved for publication
1.1	9 January 2018	P&P Project Manager	Update email address to feedback@ssi.org.au