Privacy

Settlement Services International

Privacy Management Plan

Version 2, August 2020

Table of Contents

1 OVERVIEW 3
1.1 PURPOSE 3
1.2 SCOPE 3
1.3 INTRODUCTION 3
1.4 RESPONSIBILITIES OF STAFF 4
2 PERSONAL & HEALTH INFORMATION 5
2.1 WHAT IS PERSONAL INFORMATION? 5
2.2 WHAT DOES NOT CONSTITUTE PERSONAL INFORMATION? 5
2.3 WHAT IS HEALTH INFORMATION? 5
2.4 MAIN KINDS OF PERSONAL AND HEALTH INFORMATION HELD BY SSI 6
2.5 CONFIDENTIALITY OF RECORDS 7
3 APPLYING THE PRIVACY PRINCIPLES 8
3.1 COLLECTION 8
3.2 STORAGE 9
3.3 ACCESS AND ACCURACY 10
3.4 USE 12
3.5 DISCLOSURE 13
3.6 IDENTIFICATION 14
3.7 HEALTH RECORDS LINKAGE SYSTEMS 14
3.8 EXEMPTIONS 14
4 COMPLAINTS AND BREACHES 16
4.1 COMPLAINTS 16
4.2 INTERNAL REVIEWS 16
4.3 LODGING A COMPLAINT WITH THE PRIVACY COMMISSIONER (HRIPA) 17
5 PROMOTING PRIVACY 18
5.1 STAFF TRAINING AND EDUCATION 18
5.2 PUBLIC AWARENESS 18
6 DOCUMENT CONTROL 19
6.1 RELATED DOCUMENTS 19
6.2 DOCUMENT HISTORY 19

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**) (which SSI is required to comply with as if it were a public sector agency under various NSW funding contracts);
- 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 NSW 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 sits alongside Settlement Services International's (SSI's) Privacy Policy, and applies to SSI's treatment of all personal and health information in NSW, whether it relates to a customer or client, an employee or another person (such as a contractor).

Specific programs within SSI may impose additional privacy obligations that exceed or are alternate to the SSI Privacy Policy and Privacy Management Plan, including under any relevant Privacy Codes of Practice applicable to the respective funding department. In general, all staff members are required to be aware of any privacy requirements and obligations that pertain to their particular program. Each program is responsible for documenting their specific procedures relating to privacy (in concert with SSI's Privacy Officer), and ensuring that applicable staff are made aware and follow them.

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 in NSW pursuant to PPIPA and HRIPA with reference to this plan, alongside our obligations under the *Privacy Act 1988* (Cth) and the Australian Privacy Principles (**APPs**) (which are covered by SSI's Privacy Policy).

PPIPA and HRIPA set out baseline privacy standards or 'privacy principles' which SSI must comply with, which are very similar to the APPs. 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 Privacy Officer, as well as by each program with respect to program-specific requirements.

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 working on NSW-based programs are required to comply with HRIPA, including the HPPs, when handling health information under any of those programs. Staff in certain programs are required to comply with PPIPA, including the IPPs, when handling personal information such programs. Both HRIPA and PPIPA 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 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 under NSW laws can be found at sections 4(3) and 4A of PPIPA, and regulation 5 of the *Privacy and Personal Information Protection Regulation 2019* (NSW). There are 14 exclusions to the definition of personal information under PPIPA and the regulations, including:

- information about an individual who has been deceased for more than 30 years
- information about an individual that is contained in a publicly available publication, and
- information about an individual in relation to a public interest disclosure under the NSW regime, and
- information about an individual that is obtained about them under Chapter 8 of the *Adoption Act 2000* (NSW).

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 information which may be held in connection with activities authorised under other discrete legislation (under sections 4(3) and 4A of PPIPA). If you have any specific queries about this, please contact SSI's Privacy Officer or the Legal Team.

2.3 What is health information?

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

- personal information that is 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 services to them
- other personal information collected to provide, or in providing, a health service
- other personal information about a person collected in connection with the donation of an individual's body parts, organs or body substances
- genetic information that is or could be predictive of the health of a person or their relatives or descendants, or
- healthcare identifiers.

Exclusions as to what constitutes health information pursuant to HRIPA can be found at section 5(3) of HRIPA, and are largely to those exemptions for personal information under PPIPA (per paragraph 2.2 above), plus information about a person that forms part of an employee record.

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, contractors and volunteers 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 in NSW 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
- employment and education history.

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 clients may include, but is not limited to:

- pre-arrival and post-arrival health assessments
- referrals to health services and other notes regarding the client's wishes with regards to the future provision of 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, SSI's Privacy Policy, and any program-specific requirements.

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 collection

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 reasonably 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 collection

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 and 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 (excluding health 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 (excluding health information), or
- it would be unreasonable or impracticable to collect health information from the individual, in which case we may collect health information from another source. Health information should also be collected in accordance with any guidelines issued by the NSW Privacy Commissioner.

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

IPP 3 / HPP 4 – Open Collection

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

If, in relation to health information, SSI reasonably believes that the individual is incapable of understanding the general nature of the matters identified above, SSI must take reasonable steps to ensure their authorised representative is aware of those matters,

Unless any of the exceptions apply, 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 by SSI, and who it will be held by
- the reason the information is being collected and if it is legally required or voluntary
- the parties to whom the information is usually disclosed to
- how the individual can access and correct the information being collected,
- the consequences that may apply if the individual decides not to provide that information, and

- the contact details of SSI (or those of whoever will hold the information).

SSI informs individuals of the above matters through its privacy statements, consent forms as required. Consent is a key control to ensure the individual has understood and provided informed consent.

IPP 4 / HPP 2 – Relevant Collection

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

When collecting personal and health information in NSW, 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.

SSI's divisions and programs that collect personal and health information in NSW 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 storage

An agency must store personal and health information securely, keep it no longer than necessary for its lawful use, and dispose of it securely and appropriately in accordance with any particular retention and disposal requirements. It must also take reasonable security safeguards to protect personal information from loss, unauthorised access, use, modification or disclosure, and any other misuse. Agencies must also ensure that, where personal information is required to be disclosed to any person for the service delivery, that all reasonable measures are taken to prevent unauthorised use or disclosure.

The security of personal information collected by SSI is paramount, whether this information is stored in computer networks or online systems (including in the cloud), or in paper-based form. This means that personal information must be protected from loss, 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.

Physical storage

Physical security is an important part of ensuring information is not inappropriately accessed. Many of SSI's divisions are moving to, or have already moved to, paperless solutions, to reduce or eliminate (where

possible) the use of hard-copy files. However, where SSI still holds hard-copy files (including under retention requirements), they are stored securely in locked cabinets with SSI's secure premises or are archived with secure and reputable archive service providers. Our staff also have access to secure storage spaces near their workstations to secure documents and devices which may contain personal or health information. SSI has policies in place to ensure that files containing personal or health information are not removed from SSI's premises unless specifically authorised.

Generally

SSI has comprehensive policies, procedures and processes in place that govern the use of information technology, and also how SSI will 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

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 – Transparency

An agency must take reasonable steps to provide an individual with details regarding the personal and health information the agency holds about them, why they have it, and what rights the individual has to access it. An agency must also ensure that any person can ascertain whether the agency holds personal or health information about them,

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 generally 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 about them, they should contact the organisation's Privacy Officer (privacy@ssi.org.au, (02) 8799-6700). If the organisation does hold personal or health information about that individual, 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 – Accessibility

An agency must generally allow an individual access to personal and health information held about them in NSW 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 individuals 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.

Under HRIPA, SSI is required to take reasonable steps to confirm the identity of the person making the request (and their authority if the request is being made by someone else on the individual's behalf).The NSW Information & Privacy Commission's 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 – Amendment

An agency must allow an individual to update, correct or amend personal and health information held about them where necessary to ensure that the information is accurate and that it is relevant, complete and not misleading for the purpose for which it is being used.

Providing individuals with access to, and correction of, their information ensures they 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 also have regard to the purpose for which the information was collected or is being used.

Where practicable, SSI can 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 SSI determines not to amend personal or health information in accordance with a request by the individual concerned, the individual can request that SSI attach a note to the information detailing the amendment sought.

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. Under HRIPA, SSI is required to take reasonable steps to confirm the identity of the person making the request (and their authority if the request is said to be made by an authorised representative of the individual).

3.4 Use

IPP 9 / HPP 9 – Accuracy

An agency must take reasonable steps to ensure that personal and health information is relevant, accurate, up to date, complete and not misleading 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 – Limits on use

The use of personal and health information held by the agency must be 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
- another purpose for which the individual has consented, or
- another purpose if specifically authorised by law.

A directly related secondary purpose is a purpose that is very closely related to the primary purpose for collection and would be the type of additional 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.

The NSW Information and Privacy Commission's 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 / HPP 11 - Limits on disclosure

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

Under PPIPA and HRIPA, SSI can disclose personal or health 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, for health information, the individual would reasonably expect the disclosure), or
- the individual is reasonably likely to be aware (or has been made specifically aware) that the type of information is usually disclosed to the other person or organisation, 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 (or, for health information, a serious threat to public safety), or
- the disclosure is otherwise required or authorised by law.

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, Skills and Employment (DESE) or the Department of Home Affairs (DHA) if requested under a relevant section of legislation that governs the Departments.

IPP 12 / HPP 14 - Special restrictions on disclosure (including disclosures outside NSW)

Other Sensitive information

*Under PPIPA, 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 necessary to prevent a serious or imminent threat to the life or health of a person or is otherwise required or authorised by law.

Trans-border disclosure of personal and health information

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

- the individual expressly consents to the disclosure
- 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 it is necessary to prevent a serious and imminent threat to life, health or safety of an individual (or, for health information, a serious threat to public health or safety)
- the recipient is subject to a substantially similar privacy regime to PPIPA or HRIPA as appropriate
- SSI has taken reasonable steps to bind the recipient by contract to privacy obligations equivalent to the IPPs or HPPs as appropriate, or
- it is otherwise permitted or required by legislation or any other law (including an applicable privacy code of practice).

3.6 Identification

HPP 12 – Use of identifiers

Under HRIPA, an organisation must only identify people by using unique identifiers if it is reasonably necessary to carry out the agency's functions efficiently. A government-assigned identifier may only be adopted for identification purposes if the individual has consented, or if otherwise required or authorised by law, and may only use or disclose government-assigned identifiers if it is necessary for the primary purpose or a secondary purpose authorised by HRIPA.

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, and that government-assigned identifiers are only adopted, used or disclosed in accordance with the relevant privacy legislation.

Healthcare identifiers are considered health information and so their collection, use and disclosure is subject to HRIPA.

HPP 13 – Option to remain anonymous

Under HRIPA, if lawful and practicable, individuals must be given the opportunity to remain anonymous when entering into transactions with or receiving health services from an organisation.

Where it is not unlawful or impracticable, individuals will be given the option of not identifying themselves (i.e. remaining anonymous), or of using a pseudonym (i.e. a replacement name or nickname), when dealing with SSI.

3.7 Health records linkage systems

HPP 15 – Authorised

An organisation 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 does not generally need to use health records linkage systems, but if this is required, SSI will only do so when individuals have expressly consented to their information being included on such a system.

3.8 Exemptions

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

Some examples of exemptions include:

- where the individual has expressly consented to non-compliance

- where compliance would pose a serious threat to the life or health of an individual, or, where non-compliance is necessary to prevent a serious and imminent threat to any person's life, health or safety
- use or disclosure for law enforcement purposes or investigative functions
- where non-compliance is lawfully authorised or required (including by another law)
- where compliance with collection notification requirements would prejudice the individual
- when the organisation exchanges information with public sector agencies in certain circumstances.

In addition, unsolicited information will not be considered to have been collected for the purposes of PPIPA or HRIPA.

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 (in this order):

- Contact the program or division involved and resolve the matter informally
- Contact the Privacy Officer at feedback@ssi.org.au to request an internal review (see below)
- If not resolved by SSI, then,
    - refer to the information and guidance about privacy complaints on the OAIC website, here: https://www.oaic.gov.au/privacy/privacy-complaints/ (this will be available for most, if not all, privacy concerns, including in relation to health information), or
    - in relation to health information privacy matters under HRIPA, you can alternatively contact the NSW Privacy Commissioner:
        - Office: Level 17, 201 Elizabeth Street, Sydney 2000
        - Postal address: GPO Box 7011, Sydney NSW 2001
        - Email: ipcinfo@ipc.nsw.gov.au
        - Phone: 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 (privacy@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, another law 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 SSI, 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.

In some circumstances, where a complaint relates to a service of SSI that is funded by a government department, SSI may be obligated to notify the relevant government department of the privacy complaint, and to follow any particular requirements of that department or the funding contract.

4.3 Lodging a complaint with the Privacy Commissioner (HRIPA)

A person aggrieved by the conduct of SSI in relation to HRIPA may complain directly to the NSW Privacy Commissioner. The NSW Privacy Commissioner does not have jurisdiction over SSI in relation to non-HRIPA matters and therefore cannot deal with any such complaints, however it may refer a complaint to the Commonwealth Privacy Commissioner if appropriate.

In this instance, the NSW Privacy Commissioner may conduct a preliminary assessment of a complaint before deciding whether and how to deal with the complaint. The NSW Privacy Commissioner 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) the same complaint has already been made to the Commonwealth Privacy Commissioner.

If the NSW Privacy Commissioner does decide to deal with the complaint, it will, in most cases, endeavour to resolve the complaint by conciliation.

The NSW 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).

In certain circumstances, if not resolved, the complaint may then be able to be dealt with by the NSW Civil and Administrative Tribunal.

The NSW 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
- Phone: 1800-472-679

5 PROMOTING PRIVACY

5.1 Staff training and education

SSI provides training, education seminars and e-learning 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, including program-specific training. The Code of Conduct specifically refers to the importance of protecting privacy and complying with relevant legislation.

The Privacy Officer and the SSI Legal Team 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.

5.2 Public awareness

SSI promotes public awareness of its privacy obligations by:

- the publication of this plan and its Privacy Policy on the SSI website
- maintaining a dedicated privacy page on the SSI website for all privacy resources and contacts
- delegating 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 SSI's Privacy Officer at privacy@ssi.org.au or, where applicable, the NSW 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
Phone: 1800 472 679

6 DOCUMENT CONTROL

6.1 Related Documents

Related Policies/Procedures	
CPAC.PO.01	Code of Conduct Policy
CLC.PO.07	Privacy Policy
CLC.PR.11	Data Breach Procedure
CIT.PO.01	Information Technology & Communications Policy
CPAC.PR.16	Clean Desk Procedure

References	
https://www.legislation.nsw.gov.au/#/view/act/1998/133/full	*Privacy and Personal Information Protection Act 1998 (NSW)*
https://www.legislation.nsw.gov.au/#/view/regulation/2019/391/full	*Privacy and Personal Information Protection Regulation 2019* (NSW)
https://www.legislation.nsw.gov.au/#/view/act/2002/71/full	*Health Records and Information Privacy Act 2002* (NSW)
https://www.legislation.nsw.gov.au/#/view/regulation/2017/215/full	*Health Records and Information Privacy Regulation 2017* (NSW)
https://www.ipc.nsw.gov.au/checklist-identifying-privacy-issues	Checklist - Identifying privacy issues, NSW Information and Privacy Commission
https://www.ipc.nsw.gov.au/sites/default/files/file_manager/Guide-privacy-decision-making-disabilities-ACC.pdf	Guide: Privacy and people with decision-making disabilities, Information and Privacy Commission New South Wales

6.2 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
2	1 August 2020	Legal Counsel and Privacy Officer	General review and updates in line with the legislation and internal procedures