Privacy Management Plan

Version 1.0
21/02/2018

Contents

1 Introduction

1.1 Purpose

This Privacy Management Plan (plan) explains how the NSW State Emergency Service (NSW SES) manages personal and health information under NSW privacy laws.

The NSW SES has obligations under the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act) and the *Health Records and Information Privacy Act 2002* (NSW) (HRIP Act). One of those obligations is this plan.

This plan sets out the commitment of the NSW SES to:

- protect the privacy rights of staff, volunteers, customers, clients and members of the public
- demonstrate to members of the public how the NSW SES meets its obligations under the PPIP Act and HRIP Act
- 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 NSW SES operations
- meet the requirements for NSW SES to have a plan under section 33 of the PPIP Act.

For information about the PPIP Act and the HRIP Act, please refer to Appendix A.

1.2 Scope

Section 33(2) of the PPIP Act sets out the requirements of this plan. This plan must include:

- information about how policies and practices are developed in line with the PPIP Act and the HRIP Act
- how staff are trained in these policies and practices
- internal review procedures
- anything else that is relevant to the plan in relation to privacy and the personal and health information held.

1.3 Review of this plan

This plan will be reviewed every 12 months. It will be reviewed earlier if any legislative, administrative or systemic changes affect how personal and health information is managed.

1.4 About us

1.4.1 The NSW SES

The NSW SES is an emergency service and rescue provider staffed almost entirely by volunteers established pursuant to the *State Emergency Services Act 1989* (NSW) (SES Act). The NSW SES is the combat agency for flood, storm and tsunami operations as prescribed in accordance with the *State Emergency and Rescue Management Act 1989* (NSW). The service also provides trained teams to support other emergency services as required.

1.4.1 NSW SES functions

The core functions of the NSW SES are set out in section 8 of the SES Act:

- protect persons from dangers to their safety and health and protect property from destruction or damage, arising from floods, storms and tsunamis
- act as the combat agency for dealing with floods, storms and tsunamis and to co-ordinate the evacuation and welfare of affected communities
- assist other NSW emergency service agencies in dealing with any incident or emergency.

2 Personal and health information held by the NSW SES

2.1 Types of personal and health information held

2.1.1 Members of the NSW SES (Staff and Volunteers)

The NSW SES holds a large amount of personal and health information about its members. Members include employees and volunteers. The information includes:

- personal contact details and emergency contact details (including telephone number, postal and email address)
- date of birth
- financial information (such as salary, bank account information, tax file number)
- personnel information (such as attendance records, leave balances, educational and professional qualifications, training records)
- background information (such as criminal history, ethnic background, disability)
- health information (including medical certificates, reports and files, and fitness for duty assessments)
- statements and opinions
- audio recordings of telephone conversations and interviews
- photographs/footage
- injury management information such as workplace injuries, workers compensation claims and payments and return to work plans
- secondary employment
- conflicts of interest
- location data (eg/ automatic vehicle locator tracking devices in NSW SES vehicles)
- criminal checks

2.1.2 Members of the public

The NSW SES also holds personal and health information about its customers, clients and other members of the public. Some examples of the main types of personal and health information held by clients and other members of the public include:

- name and personal contact details (including telephone number, postal and email address)
- financial information (such as bank account information)
- date of birth
- audio recordings (where incoming telephone conversations to our call centres are recorded)
- opinions (general enquiries, consultation, feedback and complaints)
- photographs/CCTV footage

The NSW SES does not maintain any public registers for the purposes of the PPIP Act or the HRIP Act.

3 Management of health and personal information

3.1 Collection

3.1.1 Collection for lawful purposes (IPP 1 & HPP 1)

Personal and health information is collected in a number of ways, including in writing, by email, through its website, over the phone, by fax, recordings (such as CCTV footage or telephone conversations) or in person. Personal and health information is only collected when it is reasonably necessary in the circumstances to collect that information.

3.1.2 Direct collection (IPP 2 & HPP 3)

The NSW SES will only collect information from a third party where:

- the person has authorised collection of the information from someone else
- the person is under 16 years of age, in which case personal information will be collected from the person's parent or guardian
- in the case of health information, it would be unreasonable or impracticable to collect information from an individual.

3.1.3 Requirements when collecting information (IPP 3 & HPP 4)

Notification is provided through a 'privacy notice'.

Notification is not required if the information is not directly collected from the individual, except in the case of health information.

3.1.4 Relevant (IPP 4 & HPP 2)

Reasonable steps are taken to ensure that information collected from an individual is not unreasonably intrusive or excessive, and is relevant, accurate, up-to-date and complete.

To determine what might be reasonable, the following is considered:

- the purpose for which the information was collected
- the sensitivity of the information
- how many people will have access to the information
- the importance of accuracy to the proposed use
- the potential effects of the individual concerned if the information is inaccurate, out-of-date or irrelevant
- the opportunities to subsequently correct the information, and
- the ease which the information can be checked.

3.2 Retention and security (IPP5 and HPP 5)

Information is stored in a variety of ways, including in databases, cloud storage, by third parties and in various physical office locations.

Reasonable security measures are maintained, including technical, physical and administrative actions, to protect information from unauthorised access and misuse.

Examples of security measures include:

- restricting access to all IT systems and databases to ensure that only authorised users with a clear business need can access them
- use of strong passwords for computer access and a mandatory requirement that all staff change computer access passwords on a regular basis
- print on demand (secured printing)
- implementing and maintaining strong security software access across all network components in arrangements for data transmission (including encryption and password protection where appropriate), backup and storage
- maintaining logs and audit trails which are monitored and retained on a regular basis
- providing staff with access to secure storage spaces near workstations to secure documents and devices
- physically securing sensitive and confidential information in locked rooms
- implementing and observing a clear desk policy
- adopting best practice in electronic and paper records management and complying with our obligations under the *State Records Act 1998* (NSW)
- keeping information for only as long as necessary
- destroying information in a secure manner as appropriate (for example, using locked recycling bins and shredders)
- where it is necessary for information to be transferred to a third party provider for the purposes of providing a service, contract terms are developed and executed to prevent unauthorised use or disclosure of information
- providing information security awareness training to NSW SES members.

3.3 Accuracy and access

3.3.1 Transparency (IPP 6 and HPP 6)

Please contact the NSW SES on the details included in Part 5 if you have any questions about the personal and health information held by the NSW SES.

3.3.2 Access to personal and health information (IPP 7 and HPP 7)

Members of the NSW SES (Staff and Volunteers)

Staff are able to access their personnel file by making a request to Member Services. Member Services can be contacted at membership@ses.nsw.gov.au.

Volunteers are able to access their member file by making a request to their relevant Region Headquarters.

Files about disciplinary matters and grievances are confidential. If you want to access your personal information on these files you will need to complete the 'Access to Own Personal Records Application' form.

Members of the public

If you would like access to your own personal records, please complete the 'Access to Own Personal Records Application' form located at www.ses.nsw.gov.au or contact us on the details included in Part 5.

Access to information under GIPA Act

Anyone is able to seek access to government information that is held by the NSW SES under the *Government Information (Public Access) Act 2009* (GIPA Act). Sometimes the information that is requested includes personal and health information of other people. There are certain considerations that are taken into account before any information of this type is released. For more information about the GIPA Act or making an access application, please visit www.ses.nsw.gov.au/about-us/access-to-information/.

3.3.3 Alterations to personal and health information (IPP 8 and HPP 8)

Members of the NSW SES (Staff and Volunteers)

Staff are able to request amendment of their personal or health information by making a request to Member Services. Member Services can be contacted at membership@ses.nsw.gov.au.

Volunteers are able to request amendment to their member file by making a request to their relevant Region Headquarters.

Members of the public

If you would like to amend your own personal records, please complete the 'Alteration of Personal Records Application' form located at www.ses.nsw.gov.au or contact us on the details included in Part 5.

3.4 Use

3.4.1 Accuracy (IPP 9 and HPP 9)

Reasonable steps will be taken to ensure that personal and health information is still relevant and accurate before it is used.

3.4.2 Limited Use (IPP 10 and HPP 10)

The NSW SES will only use personal and health information for the purpose which it was collected. That purpose is set out in the privacy notice.

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.

Some examples of where the law permits the use personal or health information for another (secondary) purpose include:

- quality assurance activities such as monitoring, evaluating and auditing
- work health and safety laws require that we use information to ensure the safety of our employees
- unsatisfactory professional conduct or breach of discipline
- the information relates to a person's suitability for appointment or employment as a public sector official
- finding a missing person
- preventing a serious threat to public health and safety.

3.5 Disclosure

3.5.1 Disclosure (IPPs 11 & 12 and HPPs 11 & 14)

Personal and health information will only be disclosed in accordance with IPPs 11 and 12 and HPPs 11 and 14, or when you have provided consent to do so or it is permitted or required to by law.

3.5.2 Identifiers (HPP 12)

Members are assigned an individual "400" member number when joining the NSW SES.

3.5.3 Anonymity (HPP 13)

This HPP is not relevant to the functions and activities of the NSW SES.

3.5.4 Linkage of Health Records (HPP 15)

Health records linkage systems will only be used when individuals have expressly consented to their information being included on such a system, or for research purposes which have been approved by an Ethics Committee.

3.6 Exemptions to how we manage personal and health information

3.6.1 Specific exemptions contained in the PPIP Act and the HRIP Act

The PPIP Act and the HRIP Act provide that compliance with some or all of the IPPs and HPPs is not necessary if certain circumstances apply.

Some examples of exemptions most relevant to the functions and activities of the NSW SES include:

- unsolicited information
- personal information collected before 1 July 2000

- health information collected before 1 September 2004
- use or disclosure for law enforcement purposes or investigative functions
- whether another law authorises or requires us not to comply
- where non-compliance is lawfully authorised or required
- where compliance would prejudice the individual
- where we exchange information with other public sector agencies
- some research purposes

3.6.2 Other legislation

The following legislation may affect how the IPPs and HPPs apply:

- *Government Information (Public Access) Act 2009* (NSW)
- *State Records Act 1998* (NSW)
- *Workplace Surveillance Act 2005* (NSW)
- *Surveillance Devices Act 2007* (NSW)
- *Ombudsman Act 1974* (NSW)
- *Public Interest Disclosures Act 1994* (NSW)
- *Telecommunications (Interception and Access) Act 1979* (Cth)
- *Workers Compensation Act 1987* (NSW)

3.7 Offences

Both the PPIP Act and the HRIP Act contain criminal offence provisions applicable to public sector officials and persons who misuse personal and health information.

NSW SES members are regularly reminded of their responsibilities under the PPIP Act and the HRIP Act and these obligations are reinforced in the Code of Conduct and Ethics.

4 If you think the NSW SES has breached your privacy

If you have any concerns about the handling of your personal or health information please contact the NSW SES directly so that these concerns can be resolved.

4.1.1 Your right of internal review

You have the right to ask for an internal review if you think your privacy has been breached.

An application for internal review must:

- be in writing
- be addressed to the NSW SES
- specify an address in Australia to which you can be notified after the completion of the review.

To apply for an internal review, you can submit the ‘Internal Review (Privacy) Application’ form or send your application and any relevant material by email or post at the details provided in Part 5.

Internal review process

The internal review will be conducted by a person who:

- was not involved in the conduct which is the subject of the complaint
- is a staff member of the NSW SES, and
- is qualified to deal with the subject matter of the complaint.

The internal review is conducted in accordance with the process set out in the Information & Privacy Commission's 'Internal Review Checklist'. When the internal review is completed, the applicant will be notified in writing of:

- the findings of the review
- the reasons for those findings
- the action we propose to take
- the reasons for the proposed action (or no action), and
- the applicant's entitlement to have the findings and the reasons for the findings reviewed by the NSW Civil and Administrative Tribunal.

A copy of your internal review request and the draft internal review report will be sent to Privacy Commissioner. Any submissions made by the Privacy Commissioner must be considered as part of the review. A final copy of the internal review decision will also be provided to the Privacy Commissioner.

Timeframes

You must lodge your request for internal review within six months from the time you first became aware of the conduct that you think breached your privacy.

The NSW SES will acknowledge receipt of an internal review and will aim to:

- complete the internal review within 60 calendar days, and
- respond to you in writing within 14 calendar days of completing the internal review.

If the internal review is not completed within 60 days, you have a right to seek a review of the conduct by the NSW Civil and Administrative Tribunal.

4.1.2 Your right to external review

You have the right to apply to the NSW Civil and Administrative Tribunal if you have sought an internal review and:

- you are not satisfied with the outcome of the internal review
- you are not satisfied with the action taken in relation to your application for internal review
- you do not receive an outcome of the internal review within 60 days.

For more information about seeking an external review, contact the Tribunal on the details below:

Office: NSW Civil and Administrative Tribunal (NCAT) – Administrative and Equal Opportunity Division – Level 10, John Maddison Tower – 86-90 Goulburn Street, Sydney NSW 2000

Phone: 1300 006 228

Website: www.ncat.nsw.gov.au

4.1.3 Complaints to the Privacy Commissioner

You have the option of complaining directly to the Privacy Commissioner if you believe your privacy has been breacked.

The Privacy Commissioner's contact details are:

Office: Information & Privacy Commission – Level 17, 201 Elizabeth Street, Sydney NSW 2000

Post: GPO Box 7011, Sydney NSW 2001

Phone: 1800 472 679

Website: ipcinfo@ipc.nsw.gov.au

5 Contact us

For further information about this plan or questions about your privacy, please contact the NSW SES on the details below:

Web: www.ses.nsw.gov.au

Post: Privacy Officer, Legal & Parliamentary Services

NSW SES

PO Box 6126

Wollongong, NSW 2500

Phone: (02) 4251 6509

Email: gipa@ses.nsw.gov.au

Appendix A – About the privacy laws

The PPIP Act and personal information

The PPIP Act sets out how personal information should be managed.

What is personal information?

Personal information is defined in section 4 of the PPIP Act and is essentially any information or opinions about a person where that person's identity is apparent or can be reasonably ascertained. Personal information can include a person's name, address, family life, sexual preferences, financial information, fingerprints and photos.

There are some kinds of information that are not personal information, e.g. information about someone who has been dead for more than 30 years, information about someone that is contained in a publicly available publication, or information or an opinion about a person's suitability for employment as a public sector official. Health information is generally excluded here as it is covered by the HRIP Act.

Information Protection Principles

Part 2, Division 1 of the PPIP Act contains 12 IPPs. Here is a summary of them:

Collection		
Lawful	1	Only collect your personal information for a lawful purpose. It must be needed for the agency's activities.
Direct	2	Collect the information from only you, unless exemptions apply.
Open	3	Tell you that the information is being collected, why and who will be using it and storing it. You must be told how to access it and make sure it's correct.
Relevant	4	Make sure that your personal information is relevant, accurate, current and non-excessive.
Storage		
Secure	5	Store your personal information securely. It should not kept longer than needed, and disposed of properly.

Access and Accuracy		
Transparent	6	Provide you with details about the personal information they are storing, reasons why they are storing it and how you can access it if you wish to make sure it's correct.
Accessible	7	Allow you to access your personal information in a reasonable time frame and without being costly.
Correct	8	Allow you to update, correct or amend your personal information when needed.
Use		
Accurate	9	Make sure that your personal information is correct and relevant before using it.
Limited	10	Only use your personal information for the reason they collected it.
Disclosure		
Restricted	11	Only release your information if you consented. An agency, however, may also release your information if it's for a related reason and can be reasonably assumed that you would not object. Or your information is needed to deal with a serious and impending threat to someone's health and safety including your own.
Safeguarded	12	Not disclose your sensitive information without your consent. Such information includes: racial, ethnic information, political, religious and philosophical beliefs, sexual activity and trade union membership. Your information may only be released without consent to deal with a serious and impending threat to someone's health and safety.

Exemptions to the IPPs

Part 2, Division 3 of the PPIP Act contains exemptions to compliance with IPPs in certain situations. For example:

- not required to comply with IPPs 2-3, 6-8, or 10-12 if lawfully authorised or required not to do so
- not required to comply with IPP 2 if the information concerned is collected in relation to court or tribunal proceedings
- not required to comply with IPP 10 if the information is used for law enforcement purposes or for the protection of public revenue.

Privacy codes of practice and public interest directions can modify the IPPs for any NSW public sector agency. These are available on the Information & Privacy Commission website (ipc.nsw.gov.au).

There are currently no public interest directions or codes of practice that are likely to affect how the NSW SES manages personal information.

Offences

Offences can be found in section 62-68 of the PPIP Act.

It is an offence for the NSW SES to:

- intentionally disclose or use personal information accessed in doing our jobs for an unauthorised purpose
- offer to supply personal information that has been disclosed unlawfully
- hinder the Privacy Commissioner or a member of staff from doing their job.

Public Registers

The PPIP Act also governs how NSW public sector agencies should manage personal information contained in public registers (Part 6 – Public Registers).

As we neither hold nor maintain any public registers this section does not apply to us.

The HRIP Act and personal information

The HRIP Act sets out how health information should be managed.

What is health information?

Health information is a more specific type of personal information and is defined in section 6 of the HRIP Act. Health information can include information about a person's physical or mental health such as a psychological report, blood test or an X-ray, or even information about a

person's medical appointment. It can also include some personal information that is collected to provide a health service, such as a name and contact number on a medical record.

Health Privacy Principles

Schedule 1 to the HRIP Act contains 15 HPPs. Here is a summary of them:

Collection		
Lawful	1	Only collect your health information for a lawful purpose. It must also relate directly to the agency's activities.
Relevant	2	Make sure that your health information is relevant, accurate, current and non-excessive.
Direct	3	Collect your health information from only you, unless exemptions apply.
Open	4	Tell you that the information is being collected, why and who will be using it and storing it. You must be told how to access it if you wish to make sure it's correct.
Storage		
Secure	5	Store your health information securely. It should not kept longer than needed, and disposed of properly.
Access and Accuracy		
Transparent	6	Provide you with details about the health information they are storing, why and how you can access it.
Accessible	7	Allow you to access your health information in a reasonable timeframe and without being costly.

Correct	8	Allow you to update, correct or amend your health information when needed. (Note: private sector organisations should also refer to s33-37 of the HRIP Act for further provisions).
Accurate	9	Make sure that your health information is correct and relevant before using it.
Use		
Limited	10	Only use your health information for the reason that is was collected, unless exemptions apply.
Disclosure		
Limited	11	Only disclose your health information for the reason that is was collected otherwise separate consent is needed from you.
Identifiers and anonymity		
Not identified	12	Can only give you an ID number if it is reasonably necessary.
Anonymous	13	Give you the option of receiving information from you anonymously, where practicable.
Transferrals and linkage		
Controlled	14	Only transfer health information outside NSW in accordance with the HPP 14.
Authorised	15	Only use health records linkage systems if you have provided consent.

Exemptions to the HPPs

Schedule 1 to the HRIP Act contains exemptions to compliance with IPPs in certain situations.

An example of an exemption is that compliance with HPPs 4-8, and 10 is not necessary if lawfully authorised, required or permitted not to comply with them.

Health privacy codes of practice and public interest directions can modify the HPPs for any NSW public sector agency. These are available on the Information & Privacy Commission website (ipc.nsw.gov.au).

There are currently no public interest directions or codes of practice that are likely to affect how the NSW SES manages health information.

Offences

Offences can be found in sections 68-70 of the HRIP Act.

It is an offence for the NSW SES to:

- intentionally disclose or use health information accessed in doing our jobs for anything else other than what we are authorised to
- offer to supply health information that has been disclosed unlawfully
- attempt to persuade a person from making or pursing a request for health information, a complaint to the Privacy Commissioner or an internal review under the PPIP Act.

Document control sheet

Title	*Privacy Management Plan*
Current Version #	1.0
Document Approval Status	Final
Directorate	Office of the Commissioner
Branch/Region/Unit/	Legal & Parliamentary Services
Guideline Owner	Manager, Legal & Parliamentary Services
Guideline Sponsor	Chief of Staff
Effective date	21/02/2018
Next Review Date	21/02/2019
Key Words	Privacy, health, personal information, health information

Version History

Version #	Creation date	Author	Summary of changes
1.0	21/02/2018	Manager, Legal & Parliamentary	Final

Approval

Name	Title	Date	Version signed off
Clarinda Campbell	Manager, Legal & Parliamentary	09/02/2018	1.0
Natasa Mitic	Chief of Staff	21/02/2018	1.0
Mark Smethurst	Commissioner	21/02/2018	1.0