Privacy Management Plan

Key points:

Fire and Rescue NSW recognises that protecting privacy is essential to maintain the confidentiality of information and to protect the privacy rights of individuals.

Under the *Privacy and Personal Information Protection Act 1998* (PPIPA) all agencies must have adequate measures in place to ensure they protect privacy. FRNSW has developed this Privacy Management Plan to support the PPIPA.

Who should read this document

Everyone in FRNSW needs to have an understanding of privacy management; however, this Plan is targeted at staff with a role in information management and will be involved in the collection, use, disclosure and storage of information.

Implementation and monitoring

This document is part of FRNSW's management of privacy risks and is supported by information management policies and procedures, which document privacy strategies.

The Governance & Legal Office reviews this document annually.

Responsible Directorate	Governance& Legal Office		
Contact	Assistant Director – Governance & Legal		
Date issued:	19 February 2015	**Version**	2

Contents

1. Overview

1.1 Purpose

This Privacy Management Plan (Plan) explains how FRNSW manages personal information in line with the *Privacy and Personal Information Protection Act 1998 (NSW)* (PPIPA) and health information in accordance with the *Health Records and Information Privacy Act 2002 (NSW)* (HRIPA).

We have a Privacy Management Plan to manage and protect the personal information FRNSW manages. The Plan also explains how to contact FRNSW about the personal and health information it holds, how information can be accessed and amended and how privacy complaints are handled.

The Plan aims to:

- meet the requirement for FRNSW to have such a plan under s 33 of the PPIPA
- demonstrate to members of the public how we meet our obligations under PPIPA and 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 customers, clients, staff and members of the public.

This plan uses plain language to describe our legal obligations and how FRNSW will comply with them. We have chosen to simplify the language in order to make our obligations easier to understand.

1.2 What this Plan covers

Section 33(2) of the PPIPA sets out the requirements of this Plan. This Plan must include:

- information about FRNSW's policies and practices to ensure compliance with the PPIPA and the HRIPA;
- how staff are made aware of these policies and practices;
- the internal review procedures,
- a requirement for all Directors to review the person information held by their divisions and confirm that they comply with the FRNSW Privacy Policy; and
- anything else considered relevant to the Plan in relation to privacy and the roll out of the protective notice of personal and health information that FRNSW holds.

1.3 When this plan will be reviewed

This Plan will be reviewed every 12 months. It will be reviewed earlier if any legislative or administrative changes affect the management of personal and health information by FRNSW.

2. Introduction

2.1 About FRNSW

FRNSW is the State Government agency responsible for the provision of fire, rescue and hazmat services in cities and towns across New South Wales in accordance with the *Fire Brigades Act 1989* , the *State Emergency and Rescue Management Act 1989* and other related legislation.

FRNSW is one of the world's largest urban fire and rescue services. Its overriding purpose is to enhance community safety, quality of life, and confidence by minimising the impact of hazards and emergency incidents on the people, property, environment and economy of NSW. More detailed information is available on FRNSW's website.

2.2 Privacy context at FRNSW

FRNSW is a 'public sector agency' for the purposes of PPIPA and HRIPA, by virtue of the definitions of 'public sector agency' provided in *s 3(1) of PPIPA* and *s 4(1) of HRIPA*. Staff collect, hold, use and disclose personal and health information for the purpose of carrying out FRNSW's functions.

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

Health information is regulated by a different set of principles set out in HRIPA. Health information is a type of personal 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*). Like the IPPs, the HPPs cover the information life cycle, but include 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. Exemptions can be found in PPIPA and HRIPA, and in regulations, privacy codes of practice and public interest directions. Where exemptions are particularly relevant to FRNSW, they have been noted in Section 4 of this plan.

2.3 Privacy management at FRNSW

All staff are responsible for complying with privacy legislation. Advice and support is available from the Privacy Officer on day-to-day privacy matters. This centralised model provides strategic management across the organisation for training, education, advisory and compliance services; coordination of forms, templates and other material provided to the public; and a single entry point for customers seeking privacy-related services or information.

2.4 Privacy Officer

The Privacy Officer acts as the focal point in FRNSW for all matters related to privacy and the handling of personal and health information.

The role of the Privacy Officer is to:

- provide advice to management, staff and business partners on privacy and the application of PPIPA and HRIPA
- provide a first point of contact for members of the public for matters related to privacy and the handling of personal and health information
- train and educate staff in aspects of PPIPA and HRIPA
- where appropriate conduct internal reviews into possible breaches of PPIPA and HRIPA
- ensure any privacy-related policies and procedures are up-to-date and are published
- develop privacy-related educational materials for staff and members of the public.

The Privacy Officer can be contacted as follows:

Post:
Privacy Officer
Governance & Legal Office
Fire & Rescue NSW
PO Box A249, Sydney South NSW 1232

Phone: 02 9265 2999
Email: info@fire.nsw.gov.au

2.5 Responsibilities of staff

Management must ensure that their staff are aware of their privacy responsibilities and any associated privacy policies, procedures, guidelines and standards, including this Plan.

All staff are required to comply with PPIPA and HRIPA, including the IPPs and HPPs when handling personal and health information held by FRNSW. Both Acts contain criminal offence provisions applicable to public sector officials and persons who misuse personal and health information; see Section 4 of this plan for more details.

This Plan aims to help staff to understand and comply with their obligations under both PPIPA and HRIPA. If staff are uncertain as to whether certain conduct may breach their privacy obligations, they should seek advice from the Privacy Officer.

Staff should identify whether any of their new projects are likely to raise any privacy issues. The Information & Privacy Commission has developed a checklist to assist staff identify when they should consult their agency Privacy Officer early in a project's design stage. Staff should complete the checklist and contact the Privacy Officer if necessary.

3. Personal and health information held by FRNSW

3.1 What is personal information?

Personal information is defined in *s 4 of PPIPA*. In summary, personal information is information or opinions that identify or could reasonably identify an individual. Common examples of personal information include a person's name, bank account details, fingerprints, a photograph or video. It can also include information that is recorded (e.g. on paper or contained in a database) and also information that is not recorded (e.g. verbal conversations). A person's identity may be apparent where neither the name nor a photograph is involved, but the information about the person is such that it could not be referring to anyone else.

Exclusions as to what constitutes personal information can be found at *ss 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
- information about an individual's suitability for 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 that is published or available on the internet. PPIPA also excludes certain information that may be held in connection with some activities authorised under different legislation.

For more information on these exclusions reference should be made to *ss 4(3)* and *4A of PPIPA* or contact made with the Privacy Officer.

3.2 What is health information?

Health information is defined in *s 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 wishes about the future provision of health services to themselves
- 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 *s 5(3) of HRIPA*. There are 15 exclusions to the definition of health information under HRIPA, which include the exclusions listed above. An example of information excluded by HRIPA is the results of a pre-employment medical check to assess a person's suitability for a job at FRNSW.

For more information on these exclusions, reference should be made to *s 5 of HRIPA* or contact made with the Privacy Officer.

3.3 Main kinds of personal and health information held by FRNSW

FRNSW has a range of functions requiring or involving the collection of personal information, including:

- providing fire, rescue and hazmat services;
- consultation with the community, businesses and other stakeholders;
- recording, investigating, and managing complaints and allegations;
- incident management;
- enforcing regulations and legislation.

Personal information may be collected by FRNSW in any of the following ways:

- personnel records;
- incident reports;
- application forms;
- financial transaction records; and
- contracts.

Personal information may be collected electronically, in writing, over the telephone or radio and in person.

FRNSW holds a range of personal and health information in a number of locations and in a range of formats. The main kinds of personal and health information held by FRNSW and a brief explanation of how those kinds of information are related to FRNSW's functions and activities are set out below:

- Personal information from persons volunteering to participate in Home Fire Safety Audits for the purposes of policy, planning and the improvement of fire safety services.
- Personal information relating to community consultation participants, such as regional forums, including details of survey responses for the purposes of research and policy development.
- Personal information for the purposes of contracting service providers.
- Personal and health information related to audit and risk works, including audit evidence collected during the performance of approved audit projects.
- Personal information collected through engagement with customers (including the broader community) to gather insights that help inform the development of policy and strategy to drive service delivery improvements.

- Personal and health information about individuals involved in incidents for the purposes of improving reporting, research and planning in support of safety strategies and policies.
- Incident records including audio recordings, images and CCTV footage for fire, rescue and hazmat incidents for the purpose of improving response, safety and community outcomes and assist insurance recovery, law enforcement and investigative agencies.
- Infringements and sanctions data to respond to traffic infringements and inform road safety policies and strategies.
- Personnel records for staff, including medical certificates, timesheets, grade and salary range and other personnel records that contain private information.

4. How FRNSW manages personal and health information

There are 12 Information Protection Principles and 15 Health Privacy Principles that FRNSW must comply with when handling personal and health information. These are summarised together below.

4.1 Collection of personal and health information – IPP1-4 & HPP1-4

FRNSW will only collect personal and health information if it is for a lawful purpose that is directly related to one of our functions and it is reasonably necessary for us to have the information.

FRNSW collects personal or health information directly from the person unless they have authorised otherwise or, in the case of health information, it would be impractical to do so.

When collecting personal or health information about an individual, FRNSW will take reasonable steps to notify the person that we are collecting that information and the purposes for which the information is being collected.

When collecting information from an individual, FRNSW 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.

4.2 Storage – IPP5 & HPP5

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

4.3 Access and accuracy – IPP6-9 & HPP6-9

FRNSW will enable anyone to know, on request to the Privacy Officer:

- whether FRNSW is likely to hold their personal and health information
- the nature of the personal and health information
- the main purposes for which FRNSW uses their personal and health information, and
- their entitlement to access their personal and health information.

FRNSW will allow people to access their personal and health information without excessive delay or expense. Access will only be refused where authorised by law. We will allow people to update or amend their personal and health information, to ensure it is accurate, relevant, up-to-date, and complete.

Before using personal or health information, FRNSW will take reasonable steps to ensure that the information is relevant, accurate, up-to-date, and complete.

4.4 Use – IPP10 & HPP10

FRNSW 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 person has consented.

4.5 Disclosure – IPP11& 12 and HPP11 - 15

FRNSW may disclose personal and health information if:

- the disclosure is directly related to the purpose for which the information was collected, and Fire & Rescue has no reason to believe that the individual concerned would object to the disclosure;
- the individual has been made aware that this kind of information is usually disclosed to the recipient;
- the disclosure is reasonably necessary to prevent or lessen a serious and imminent threat to life or health.

Higher protections are afforded to sensitive personal information. Such information includes: racial, ethnic information, political, religious and philosophical beliefs, sexual activity and trade union membership. FRNSW can generally only disclose sensitive personal information when the person has consented to the disclosure or when it is necessary to prevent a serious and imminent threat to life or health.

In terms of health information, FRNSW will only identify individuals by using unique identifiers if it is reasonably necessary for us to carry out our functions, does not currently use a health records linkage system or usually transfer health information outside NSW.

4.6 Exemptions

Exemptions to the IPPs and HPPs are discussed in a general way below. Different exemptions may apply between an IPP and its equivalent HPP. If in doubt, the wording of the exemptions contained within PPIPA and HRIPA should be consulted, and guidance sought from the Privacy Officer or Privacy Commissioner.

The exemptions include:

- unsolicited information if it contains personal information
- personal information collected before 1 July 2000
- health information collected before 1 September 2004
- personal information used for law enforcement or investigative purposes.

FRNSW may not be required to comply with some principles if lawfully authorised or required not to do so, or to lessen or prevent a serious threat to public health or safety.

4.7 Public interest directions

Under section 41 of the PPIPA, the Privacy Commissioner has made Public Interest Directions to waive or modify the requirement for a public sector agency to comply with an IPP.

Public interest directions may permit FRNSW:

- to be exempt from some principles in relation to the conduct of investigations;
- to be exempt from some principles when transferring enquiries to another NSW public sector agency;
- to disclose personal information collected for research purposes.

4.8 Memoranda of understanding

FRNSW has a number of Memoranda of Understanding (MOU) and other agreements with various bodies for access to personal information. These MOUs provide a degree of assurance that information is accessed, stored, maintained and disclosed for an agreed purpose within the terms of the MOU or agreement.

A number of relevant MOUs are published on FRNSW's intranet and website and in the agency's Annual Report; further details about relevant MOUs are available from the Privacy Officer.

4.9 Privacy codes of practice

PPIPA and HRIPA permit the development of privacy codes of practice by an agency that may modify the application of an IPP, HPP or public register provision. At the time of this Plan's publication, a privacy code of practice or health privacy code of practice has not been developed by FRNSW.

4.10 Public registers

Part 6 of PPIPA prescribes special rules for personal and health information held on public registers. These rules regulate when personal or health information contained in a public register can be disclosed. FRNSW does not maintain any public registers for the purposes of PPIPA or HRIPA.

4.11 Offences

Both PPIPA and HRIPA contain criminal offence provisions applicable to public sector officials and persons who misuse personal and health information.

The table below summarises these offences.

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 PPIPA s 68 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 s 69 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: • willfully obstruct, hinder or resist the Privacy Commissioner or a member of the staff of the Privacy Commissioner • refuse or willfully fail to comply with any lawful requirement of the Privacy Commissioner or a member of the staff of the Privacy Commissioner, or • willfully 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 ($1,100).	s 68(1) of PPIPA

5. Privacy and other legislation relating to personal and health information

5.1 Privacy legislation

- *Privacy and Personal Information Protection Act 1998* (NSW)
- *Health Records and Information Privacy Act 2002* (NSW)
- *Privacy and Personal Information Protection Regulation 2005* (NSW)
- *Health Records and Information Privacy Regulation 2012* (NSW)
- Privacy Codes of Practice, Directions and Statutory Guidelines made under PPIPA and HRIPA

5.2 Other relevant legislation and policy

Other legislation that may also affect the application of the privacy principles includes, but is not limited to:

- *Criminal Records Act 1991* (NSW)
- *Independent Commission Against Corruption Act* (NSW)
- *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 Act 1997*
- *Telecommunications (Interception and Access) Act 1979* (Cth)
- *Digital Information Security Policy**

The **Digital Information Security Policy** establishes the digital information security requirements for the NSW public sector, including the requirement to have an Information Security Management System that takes into account a minimum set of controls, and requirements relating to certification, attestation and the establishment of the Digital Information Security Community of Practice.

6. How to access and amend personal and health information held by FRNSW

6.1 Request to access and amend

People wishing to access or amend personal and health information FRNSW holds about them should contact the member of staff or unit holding the information.

The request should:

- include name and contact details
- state whether the application is made under PPIPA (personal information) or HRIPA (health information)
- explain what personal or health information is to be accessed or amended
- explain how the personal or health information is to be accessed or amended.

6.2 Limits on accessing or amending information

FRNSW is prohibited from providing access to another person's personal and health information. However:

- under section 26 of the PPIPA, a person can give FRNSW consent to disclose their personal information to someone that would not normally have access to it
- under sections 7 and 8 of the HRIPA, an "authorised person" can act on behalf of someone else
- FRNSW may be authorised to disclose health information, such as in the event of a serious and imminent threat to the life, health and safety, to find a missing person or for compassionate reasons.

7. Privacy complaints and reviews

A person who wishes to make a complaint or request a review in relation to privacy may:

- resolve the matter informally
- contact the Privacy Commissioner
- apply for an internal review by FRNSW.

7.1 Resolving the matter informally

FRNSW encourages people to try to resolve privacy concerns FRNSW informally or at least contact the Privacy Officer to discuss the issue, before lodging an application for internal review.

7.2 Privacy Commissioner

Privacy complaints may be made directly to the Privacy Commissioner. Complaints directed to the Privacy Commissioner can only result in conciliated outcomes.

Contact details for the Information and Privacy Commission are:

Email: ipcinfo@ipc.nsw.gov.au

Phone: 1800 472 679

7.3 Internal review

Individuals have the right to seek an internal review under Part 5 of the PPIPA if they think that FRNSW has breached the PPIPA or HRIPA relating to their own personal and health information. Individuals cannot seek an internal review for a breach of someone else's privacy, unless they are authorised representatives of the other person.

7.3.1 Internal review process

Applications for an internal review must be made within six months from when the applicant first became aware of the matter. Applications must be made in writing and addressed to FRNSW's Privacy Officer.

The Privacy Officer will conduct the internal review unless a conflict exists. In this case another person will be appointed to conduct the internal review.

FRNSW will:

- acknowledge receipt of an internal review within 5 working days;
- complete an internal review within 60 calendar days.

FRNSW will inform the applicant of the progress of the internal review and will respond in writing within 14 calendar days of determining the internal review.

If an applicant is not notified of the outcome of an internal review within 60 days, the applicant may seek an external review.

7.3.2 The Privacy Commissioner's role in internal reviews

FRNSW will notify the Privacy Commissioner of internal reviews. The Privacy Commissioner is entitled to make submissions to FRNSW regarding internal reviews.

7.3.3 External review by the NSW Civil & Administrative Tribunal

An applicant may seek an external review by the NSW Civil & Administrative Tribunal (NCAT).

The time frame is as follows:

1. If the internal review was completed within 60 days, then the time frame for applicants seeking to make an application to the Tribunal for a review of a privacy matter is **28 calendar** days after the day on which the applicant was notified of the result of the internal review.

2. If the internal review **was not** completed within 60 days, then the time frame for applicants seeking to make an application to the Tribunal for a review of a privacy matter is **28 calendar days** after the **later** date of either:
   a) when the applicant was notified of the result of the internal review, or
   b) the day on which the 60 day period expires.

Contact details for the NSW Civil & Administrative Tribunal are:

Phone: 1300 006 228

8. Promoting privacy

FRNSW reinforces compliance with the PPIPA and HRIPA by:

- endorsing this Plan and making it publicly available;
- providing a copy of this Plan to relevant oversight bodies such as the FRNSW Audit and Risk Committee;
- reporting on internal reviews to the Information and Privacy Commission; and
- identifying privacy issues when implementing new systems, services and processes.

FRNSW promotes awareness of privacy obligations among staff by:

- publishing FRNSW's Privacy Management Plan and privacy-related policies on FRNSW's intranet and website;
- publishing information about privacy on FRNSW's intranet;
- communicating regularly with staff about privacy;
- ensuring contractors engaged by FRNSW are aware of their privacy obligations;
- ensuring FRNSW policies comply with privacy legislation;
- including the Plan in induction packs; and
- offering training and advice to staff.

8.1 Public awareness

This Plan provides information to members of the public about how FRNSW manages personal and health information. The Plan is publicly available as open access information under the GIPA Act.

FRNSW promotes public awareness of FRNSW's Privacy Management Plan by:

- publishing the Plan on FRNSW's website;
- providing hard copies of the Plan free of charge on request;
- translating the Plan into other languages on request; and
- informing people about the Plan when responding to enquiries about personal and health information.

Annexure A

Privacy Protection Notice

Under section 10 of the *Privacy and Personal Information Protection Act 1998 (NSW)* (PPIPA), when FRNSW collects personal information from an individual, such as their name, address, telephone number or email address, FRNSW must make the individual aware of:

- the purposes for which the information is being collected;
- the intended recipients of the information;
- whether the supply of the information is required by law or is voluntary;
- any consequences for the individual if the information (or any part of it) is not provided;
- ways the individual can access and correct the information; and
- the name and address of the unit that is collecting the information and the unit that is to hold the information.

FRNSW's Privacy Protection Notice appears below:

PRIVACY PROTECTION NOTICE

Purpose of collection: *state the purposes for which the information is being collected*

Intended recipients: *to whom (including business units or organisations) the information will be disclosed*

Supply: *whether the supply of the information is required by law or is voluntary and any consequences for the individual if the information (or any part of it) is not provided*

Access/ Correction: *how the individual can access and correct the information*

Storage: *the name and address of the business unit that is collecting the information and the business unit that is storing the information.*

The Privacy Protection Notice will be introduced and progressively included on requests for personal information from individuals.