Privacy Management Plan

New South Wales Crime Commission

Contents

1. Purpose

This Privacy Management Plan explains how the New South Wales Crime Commission (the Commission) complies with its obligations under the *Privacy and Personal Information Protection Act 1998* (the PPIP Act) and the *Health Records and Information Privacy Act 2002* (the HRIP Act) (collectively the "Privacy Acts"). All Commission staff have an obligation to comply with the Privacy Acts in the course of collecting, managing, using, disclosing and securing personal and health information.

The Commission is required to prepare and implement a Privacy Management Plan in accordance with section 33 of the PPIP Act.

2. Functions of the Commission

The Commission plays a central role in the disruption of organised and other serious crime in New South Wales. Commission staff work with law enforcement partner agencies to achieve the aims of the *Crime Commission Act 2012* (the CC Act) and the *Criminal Assets Recovery Act 1990.*

The Commission is vested with statutory powers including the power to summons witnesses and take evidence, and to issue notices for the production of information, documents or things.

3. The PPIP Act

The PPIP Act provides for the protection of personal information held by government agencies and imposes obligations on those agencies in the collection, storage, access, accuracy, use and disclosure of personal information. Under the PPIP Act, *personal information* is any information or opinions about a person where that person's identity is apparent or can be reasonably ascertained from the information or opinion. Examples of personal information include a person's name, bank account details, a photograph or video. Personal information also includes such things as an individual's fingerprints, voice recordings, body samples or genetic characteristics.

4. The HRIP Act

The purpose of the HRIP Act is to promote fair and responsible handling of health information by:

- Protecting the privacy of an individual's health information held in the public and private sectors;
- Enabling individuals to gain access to their health information; and
- Providing an accessible framework for the resolution of complaints regarding the handling of health information.

Health information is defined in the HRIP Act as:

a) Personal information that is information or an opinion about:
   (i) the physical or mental health or a disability (at any time) of an individual; or
   (ii) an individual's express wishes about the future provision of health services to him or her; or
   (iii) a health service provided, or to be provided, to an individual; or
b) Other personal information collected to provide, or in providing, a health service; or
c) Other personal information about an individual collected in connection with the donation, or intended donation, of an individual's body parts, organs or body substances; or
d) Other personal information that is genetic information about an individual arising from a health service provided to the individual in a form that is or could be predictive of the health (at any time) of the individual or of a genetic relative of the individual; or

e) Healthcare identifiers, but does not include health information, or a class of health information or health information contained in a class of documents, that is prescribed as exempt health information for the purposes of the HRIP Act generally or for the purposes of specified provisions of the HRIP Act.

5. The IPPs and HPPs

The IPPs and HPPs regulate the collection, storage, use, disclosure, amendment and disposal of personal and health information. The principles also give members of the public a right to request access to their personal or health information or to ask for amendments to that information to ensure it is accurate.

The Commission is only required to comply with the IPPs in connection with the exercise of its administrative and educative functions.[1] Similarly, the HRIP Act does not apply to the Commission, except in connection with the exercise of its administrative and educative functions.[2]

As a general rule, if personal or health information is collected, stored, or disseminated for a purpose relating to the Commission's administrative or educative functions, then the IPPs and HPPs apply, and the procedures in this Privacy Management Plan must be followed. If the information is collected, stored, or disseminated for other purposes (such as investigation, misconduct prevention or law enforcement) then the IPPs and HPPs do not apply.

5.1 The Information Protection Principles

The IPPS only apply when the Commission is exercising its administrative or educative functions.

Collection	
1. Lawful	The Commission will only collect personal information for a lawful purpose, which is directly related to the agency's function or activities and necessary for that purpose.
2. Direct	The Commission will only collect personal information directly from the person concerned, unless they have authorised collection from someone else, or if the person is under the age of 16 and the information has been provided by a parent or guardian.
3. Open	The Commission will inform people why their information is being collected, what it will be used for, and to whom it will be disclosed. The Commission will tell people how they can access and amend their personal information and the consequences if they decide not to give their personal information to us.
4. Relevant	The Commission will ensure that the personal information is relevant, accurate, is not excessive and that the collection does not unreasonably intrude into the personal affairs of the individual.
Storage	
5. Secure	The Commission will store personal information securely, keep it no longer than necessary and dispose of it appropriately. It should also be protected from unauthorised access, use, modification or disclosure.
Access and accuracy	
6. Transparent	The Commission is transparent about the personal information being stored, why it is being used and about the right to access and amend it.

[1] Section 27 of the PPIP Act. A 'function is defined in both the PPIP Act and the HRIP Act to include a power, authority or a duty.
[2] Section 17 of the HRIP Act.

7. Accessible	The Commission allows people to access their personal information without excessive delay or expense.
8. Correct	The Commission allows people to update, correct or amend their personal information where necessary.
Use	
9. Accurate	The Commission will ensure that the personal information is relevant, accurate, up to date and complete before using it.
10. Limited	The Commission will only use personal information for the purpose it was collected unless the person has given their consent, or the purpose of use is directly related to the purpose for which it was collected, or to prevent or lessen a serious or imminent threat to any person's health or safety.
Disclosure	
11. Restricted	The Commission will only disclose personal information with a person's consent or if the person was told at the time that it would be disclosed, if disclosure is directly related to the purpose for which the information was collected and there is no reason to believe the person would object, or the person has been made aware that information of that kind is usually disclosed, or if disclosure is necessary to prevent a serious and imminent threat to any person's health or safety.
12. Safeguarded	The Commission cannot disclose sensitive personal information without a person's consent, for example, information about ethnic or racial origin, political opinions, religious or philosophical beliefs, sexual activities or trade union membership. It can only disclose sensitive information without consent in order to deal with a serious and imminent threat to any person's health or safety.

5.2 The Health Privacy Principles

The HPPs only apply when the Commission is exercising its administrative or educative functions.

Collection	
1. Lawful	The Commission will only collect health information for a lawful purpose that is directly related to its activities and necessary for that purpose.
2. Relevant	The Commission will ensure health information is relevant, accurate, up-to-date and not excessive, and that the collection does not unreasonably intrude into the personal affairs of a person.
3. Direct	The Commission will only collect health information from the person concerned, unless it is unreasonable or impracticable to do so.
4. Open	The Commission will inform a person as to why it is collecting health information, what the Commission will do with it, and who else may see it. The Commission will tell the person how they can view and correct their health information and any consequences that will occur if they decide not to provide their information to it. If the Commission collects health information about a person from a third party the Commission must still take reasonable steps to notify the person that this has occurred.
Storage	
5. Secure	The Commission will ensure the health information is stored securely, not kept any longer than necessary, and disposed of appropriately.

	Health information should be protected from unauthorised access, use or disclosure.
Access and accuracy	
6. Transparent	The Commission will explain to the person what health information is being stored, the reasons it is being used and any rights they have to access it.
7. Accessible	The Commission will allow a person to access their health information without unreasonable delay or expense.
8. Correct	The Commission will allow a person to update, correct or amend their personal information where necessary.
9. Accurate	The Commission will ensure that the health information is relevant and accurate before using it.
Use	
10. Limited	The Commission will only use health information for the purpose for which it was collected or for a directly related purpose, which a person would expect. Otherwise, the Commission would generally need the person's consent to use the health information for a secondary purpose.
Disclosure	
11. Limited	The Commission will only disclose health information for the purpose for which it was collected, or for a directly related purpose that a person would expect. Otherwise, the Commission would generally need the person's consent.
Identifiers and anonymity	
12. Not identified	The Commission will only identify people by using unique identifiers if it is reasonably necessary to carry out its functions efficiently.
13. Anonymous	The Commission will give the person the option of receiving services from the Commission anonymously, where this is lawful and practicable.
Transferrals and linkage	
14. Controlled	The Commission will only transfer health information outside NSW in accordance with HPP 14.
15. Authorised	The Commission will only use health records linkage systems if the person has provided or expressed their consent.

6. Information the Commission Collects

As noted earlier, the Commission is only required to comply with the IPPs in connection with the exercise of its administrative and educative functions.[3] Similarly, the HRIP Act does not apply to the Commission, except in connection with the exercise of its administrative and educative functions.[4]

The Commission limits its collection of personal information in relation to the exercise of its administrative and educative functions where appropriate and ensures that it only collects information where it is reasonably necessary to pursue its legitimate functions and activities. This section contains an outline of the personal information that is collected by the Commission and why the collection is necessary.

[3] Section 27 of the PPIP Act. A 'function is defined in both the PPIP Act and the HRIP Act to include a power, authority or a duty.
[4] Section 17 of the HRIP Act.

The Commission must make every effort to ensure that health and personal information is accurate before using it.

The manner in which Commission staff members collect and deal with personal information is governed by internal policies and procedures, in addition to the requirements of the CC Act and any other applicable laws.

Personal information may be collected in writing, using photographs or video surveillance and through electronic means. The Commission's *Workplace Surveillance Policy and Procedures* describes the kinds of surveillance that may be in use and restrictions on the use and disclosure of surveillance records. Signage in the reception area of the building alerts visitors and staff that CCTV camera surveillance may be in operation.

6.1 Commission Employees

6.1.1 Administrative Information

The Commission collects personal and health information from staff, usually for administrative purposes, such as through recruitment and people and culture management practices (e.g. proof of vaccinations, medical certificates as required by the Commission's *Sick Leave Policy and Procedures* and information relating to worker's compensation claims), vetting of prospective employees and building management/security purposes.

New employees undergo an induction program upon commencement. The induction program includes the requirement that new starters complete set readings[5] of policies and procedures, including those that relate to the collection, handling, storage of and access to personal and health information. On day one the new starter is provided with the Commission's *Health Records and Information Privacy Notice* (see Annexure A).

New employees are asked to provide a range of personal information for administrative purposes.

Staff are asked to complete Equal Employment Opportunity (EEO) forms upon commencing employment at the Commission. Disability information is used by the People &Culture Manager for the purpose of making any necessary adjustments to the workplace. The EEO forms are provided to the Finance Team for the purpose of preparing workforce profile statistics, which must be reported in the Commission's annual reports.

Employees' Tax File Numbers are retained on a separate file held securely by the Finance Team.

Commission staff have access to the majority of their own personal information, including payslips, leave balances, bank account details, superannuation information etc., which is held in the Commission's HR database and their Shared Staff Management File which includes personal information relating to Performance Development Plans (PDP), timesheets and staff training.

6.1.2 Security Vetting

The sensitivity of the information the Commission holds and accesses requires that all Commission officers must have, and retain, appropriate security clearances.

A large amount of personal information is collected from employees for the purpose of conducting background and integrity checks. Employees are required to provide this information in a standardised format and provide supporting documentation such as proof of identity (certified copies of passports, citizenship certificates, driver licences, etc.), and proof of education (academic transcripts, certificates, etc.). The standardised forms contain notifications to prospective employees, requesting consent, and also advising how their personal information and health information is being collected, how it will be used and how the information will be

[5] *Reference Materials for New Employees and New Employee Induction Checklist Week by Week Readings*

stored and retained by the Commission. The forms also contain declarations requiring applicants to confirm that the information they are providing is accurate and correct, as it will be used by the Commission to undertake checks without further reference to the applicant/employee.

Vetting information is collected for both Commission clearances and for Commonwealth security clearances. Third party information, including for example, verification of employer references and confirmation of prior employment, posts made by a prospective applicant on social media, and verification checks undertaken with universities and other academic institutions, are collated in order to substantiate claims made by employees.

All vetting information, obtained as part of the Commission's vetting procedures, is dealt with in accordance with the Privacy legislation and is only accessible by a small number of Commission officers[6]. The CC Act itself also contains safeguards relating to the use of vetting information.

6.1.3 Employee Shared Management File

The Employee Shared Management File is accessible to the relevant staff member and manager, and the People & Culture Manager and People & Culture Team, which may contain any of the following:

- Employment Agreement;
- PDP;
- Policy Awareness forms;
- Staff Variations;
- Notification of Overseas Travel forms; and
- Learning nomination forms.

6.1.4 Human Resources Personnel Files

Human Resources Personnel Files are accessible to the People & Culture Team, the Chief Operating Officer and the Finance Team, and may contain any of the following:

- New Starter induction;
- Payroll;
- Probation;
- Employment Agreement;
- Staff variation forms;
- Letters of offer; and
- File notes.

6.1.5 Personnel Security file

This file may contain the employee's vetting application and results of vetting checks. This file is only accessible to the Personnel Security Team and Chief Operating Officer.

6.1.6 Salaries file

This file is maintained by the Finance Team and stored securely. The salaries file may contain any of the following (but is not limited to):

- Salary details;
- Bank details;
- Superannuation;
- New starter details; and
- Salary sacrifice.

6.1.7 Leave file

The leave file is maintained by Finance Team and stored securely in accordance with the Commission's record-keeping policy. The leave file may contain leave applications and medical certificates.

6.1.8 Commonwealth security vetting

An employee's Personal Security file may also contain a copy of the completed application, the clearance letter and a copy of the Vetting Manager's email advising the staff member of the results of their clearance application.

6.1.9 Medical Certificates

Medical certificates are placed on the employee's personal file. The circumstances under which a medical certificate may be required are contained in the Commission's *Sick Leave Policy and Procedures* and *Carer's Leave Policy and Procedures.*

6.2 Visitors

The Commission collects limited information from visitors to the Commission building, including their name, organisation, photograph and the purpose of their visit. Visitors are required to provide this information to the Commission electronically and this facility contains a notice about the use of the personal information collected, as well as camera surveillance that is operated onsite. Visitors, when signing into the Commission, must complete a form and are provided with a disclaimer indicating how their personal information is collected, and how it may be accessed and/or amended.

6.3 Information Related to Commission Functions

The Commission collects information in relation to its law enforcement functions, including:

- Investigation of criminal offences and general intelligence gathering;
- Serving or answering subpoenas;
- Financial forensic analysis;
- General intelligence gathering;
- Controlled operations;
- Witness protection;
- Informant management; and
- Obtaining assets forfeiture orders or proceeds assessment orders.

Generally, the IPPs do not apply to the collection of this information.

6.4 Anonymous Collection of Information

Wherever it is lawful and practicable, the Commission will give people the opportunity to remain anonymous when dealing with the Commission. Generally, due to the Commission's functions, it will be impracticable to deal with an individual anonymously due to the type of personal information required from an individual as part of the recruitment and/or employment process, such as:

- Personal contact details;
- Employment details;
- Financial details; and
- Bank account/credit card details.

Complaints made about the Commission and/or a Commission officer can be made anonymously and will be assessed by the Commission where there is sufficient information provided to do so.

7. Security and Destruction of Information

The Commission building is secure and access to each floor is granted only according to need. Within these secure areas, all personal and health information retained is stored in locked cabinets. Only those with a need to know have access to personal and health information.

In accordance with records management legislation, the Commission's *Records and Information Management Policy and Procedures* and the Commission's destruction/retention schedules, all records are retained, handled and destroyed securely. Personal information will only be retained by the Commission for as long as it may be used for legitimate purposes in connection with its functions.

8. Access to Information

Commission officers have the right to access their personal and health information, and to update and amend that information as appropriate. Commission officers should first make any relevant amendments through the HR database. If this is not possible, he or she should subsequently make any such request through the People & Culture Manager and the People & Culture Manager must comply with the request without delay. Access to certain files is only permitted in the company of the People & Culture Manager or other appropriately senior officer.

The Commission's *Change of Circumstances Notification* allows an employee to update many kinds of information and reminds employees of their obligation to advise such changes of circumstance.

If people outside of the Commission (not including former staff members) require access to their personal information which the Commission holds, they should first forward an initial request to the Commission's Privacy Officer The Commission's Privacy Officer may be able to deal with the request informally. If the matter cannot be dealt with informally, the individual can apply for such information under the *Government Information (Public Access) Act 2009* (GIPA Act), as nothing in the PPIP Act affects the operation of the GIPA Act. The Commission may still refuse to provide such information, or deem any such application as invalid, in accordance with the provisions of the GIPA Act.

9. Use of Information

The Commission takes 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.

Commission staff are periodically reminded to update their personal details contained in the HR database, and can also update personal information about themselves, such as emergency contact details, banking details and other contact details, at their convenience.

Prior to using personal information, the Commission will take reasonable steps to test its accuracy, by considering the following (as relevant):

- The purpose for which the information was collected;
- When the information was collected, and whether more current information can be obtained;
- The purpose for which the information is being used;
- How important the accuracy of the information is;
- The impact on the individual if the information is inaccurate, out of date; or
- Whether there are any other ways to corroborate and/test the accuracy of the information.

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

10. Disclosure of Information

The Commission will not disclose personal information, unless the person has consented to the disclosure or the law permits or requires the Commission to disclose it.

Under the PPIP Act, the Commission can disclose personal information for a secondary purpose if:

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

The Commission also has a discretion to, and can be required to, disclose information to other law enforcement agencies in relation to law enforcement, including for example:

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

11. Commission Policies

The Commission develops policies in compliance with the PPIP Act and the HRIP Act.

There are a number of Commission policies which relate to how the Commission deals with personal and health information. These include the:

- Code of Conduct;
- Complaints handling policy and procedures;
- Accessing operational databases policy and procedures;
- Commission website data collection privacy policy;
- Workplace surveillance policy and procedures ; and
- Information security policy;

All Commission policies are available to staff through the Commission's intranet. Where possible, these policies have been made publicly available to members of the public on the Commission's website.

12. Data Breaches and the Mandatory Notification of Data Breach Scheme

The Commission has developed a Data Breach Policy which sets out the practices and and procedures in place for responding to a data breach.

These procedures include assessment, containment, and mandatory reporting of data breaches.

All Commission staff should be familiar with the practices and procedures set out within the Data Breach Policy. This policy is available on the Commission intranet and the Commission website.

13. Complaints and Breaches

The Commission is committed to protecting the privacy of personal and health information in accordance with the Privacy Laws.

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

- Contact the relevant person/unit involved and resolve the matter informally;
- Apply for an internal review; and/or
- Contact the Privacy Commissioner.

Lodging an application for internal review

Any person who believes the Commission has misused their personal or health information can lodge an application for internal review. Complaints can be made using the *Privacy Complaint: Internal Review Application Form* (see Annexure B), however, internal review applications may be lodged in other written formats.

The Commission, after receipt of such an application, will conduct an internal review to determine:

- whether or not the alleged conduct occurred;
- if so, whether the Commission complied with its privacy obligations;
- if not, whether non-compliance was authorised by an exemption; and/or
- appropriate action (if any) by way of a response and/or remedy.

Once the Commission completes its internal review, the Commission will advise the person aggrieved and the Privacy Commissioner of its findings (if any) and any actions taken as a result of the internal review.

The Commission is required to follow the requirements set out in Part 5 of the PPIP Act when carrying out an internal review, whether the conduct relates to an alleged breach of the PPIP Act or the HRIP Act. The Privacy Contact Officer will refer to the Privacy Commissioner's guidance materials when carrying out an internal review, in particular *A guide for conducting internal reviews* and the *Internal review checklist* on the NSW Privacy Commissioner's website.

The role of the NSW Privacy Commissioner in relation to internal reviews

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

In conducting internal reviews about personal or health information, the Commission, in compliance with the Privacy Laws, must:

- Notify the NSW Privacy Commissioner that they have received the application for internal review;
- Keep the NSW Privacy Commissioner informed of the progress of the internal review;
- Consider any relevant material submitted by the applicant or by the NSW Privacy Commissioner;
- Complete the review as soon as possible (and in any case, the Commission must complete the review **within 60 days** of receipt);
- Once the review is finished, notify the applicant and the NSW Privacy Commissioner of the findings of the review (and the reasons for those findings), and the action proposed to be taken; and/or
- Notify the applicant of their right to have those findings, and the agency's proposed action, reviewed by the New South Wales Civil and Administrative Tribunal (the NCAT).

If the internal review is not completed within 60 days from the date the application was received or that person is dissatisfied with the Commission's findings, then the complainant has 28 days to make an application under section 55 of the PPIP Act to the NCAT for the review of the conduct or decision complained about.

Lodging a complaint directly with the NSW Privacy Commissioner

Alternatively, a complaint made be made to (or by) the NSW Privacy Commissioner about the alleged violation of, or interference with, the privacy of an individual. The NSW Privacy Commissioner must undertake a preliminary assessment of any privacy-related complaint, and may decide not to deal with a complaint if the NSW Privacy Commissioner is satisfied that:

- The complaint is frivolous, vexatious or lacking in substance, or is not in good faith;
- The subject matter of the complaint is trivial;
- The subject matter of the complaint relates to a matter permitted or required by or under any law;
- There is available to the complainant an alternative, satisfactory and readily available means of redress; and/or
- It would be more appropriate for the complainant to make an application for internal review under section 52 of the PPIP Act.

14. Education and Awareness

The Commission promotes awareness of the Privacy Laws by:

- Endorsing this plan by making it publicly available;
- Development of information management and cyber security related training;
- Incorporating privacy related information as part of the Commission staff induction;
- Identifying privacy issues when implementing new systems, services and processes, and ensuring the Commission's policies comply with privacy legislation;
- Making Commission staff aware of the Commission's privacy obligations by developing privacy training courses and/or materials that supplement mandatory information and cybersecurity training

15. Role of Nominated Privacy Officer

The Commission has nominated a dedicated Privacy Officer reporting to the Chief Operating Officer to manage privacy related issues including:

- Providing internal privacy advice
- Providing / assisting with the completion of Privacy Impact Assessments
- Managing the Commission's response to data breaches
- Completing or coordinating privacy audits
- Drafting and reviewing privacy documentation
- Review existing or proposed arrangements with contracted service providers
- Coordinating privacy awareness training
- Handling privacy complaints received by the Commission
- Liaising with privacy regulators regarding data breach notifications

16 Offences and Penalties

Part 8 of the PPIP Act and the HRIP Act detail various penalties for offences under the Privacy Acts.

The relevant provisions are set out below in further detail:

Legislative provision/s	Details	Maximum penalty
• Section 62(1) of the PPIP Act • Section 68(1) of the HRIP Act	It is an offence for a public sector official[7] to corruptly disclose and/or use personal and health information.	100 penalty units or imprisonment for 2 years, or both

[7] A public sector official refers to any person who is employed or engaged by a public sector agency. In this section, it is noted that a public sector official includes a reference to a person who was formerly a public sector official.

• Section 62(2) of the PPIP Act • Section 68(2) of the HRIP Act	It is an offence for any person to induce or attempt to induce a public sector official (by way a bribe or other corrupt conduct) to disclose personal and healthy information.	100 penalty units or imprisonment for 2 years, or both
• Section 63 of the PPIP Act • Section 69 of the HRIP Act	It is an offence for a person to offer to supply personal or health information that has been disclosed unlawfully.	100 penalty units or imprisonment for 2 years, or both
Section 70(1) of the HRIP Act	It is an offence for a person to (by threat, intimidation or misrepresentation) persuade or attempt to persuade an individual to: • refrain from making or pursuing a request to access health information; • making a complaint to the NSW Privacy Commissioner; • making an application for internal review • withdraw any such request, application or complaint.	100 penalty units
Section 68(1) of the PPIP Act	It is an offence for a person to hinder or obstruct any staff member of the NSW Information and Privacy Commission in the exercise of his or her functions under the PPIP Act and/or the HRIP Act.	10 penalty units

In addition to the above, section 80 of the CC Act provides that Commission staff (current and former) must not, directly or indirectly, except for the purposes of the CC Act or in connection with his or her functions under the CC Act: make a record of any information or divulge or communicate to any person any information which was acquired because of, or in the course of, exercising his or her functions under the Act. The maximum penalty for this offence is 50 penalty units or imprisonment for 12 months, or both.

17. Contacts

Current contact details as follows:

NSW Crime Commission Privacy Contact Officer governmentinformationofficer@crimecommission.nsw.gov.au NSW Crime Commission (02) 9269 3888	
NSW Civil and Administrative Tribunal 1300 006 228 www.ncat.nsw.gov.au PO Box K1026, Haymarket NSW 1240	**NSW Information and Privacy Commission** 1800 472 679 ipcinfo@ipc.nsw.gov.au GPO Box 7011, Sydney NSW 2001

Level 9, John Maddison Tower, 86-90 Goulburn Street, Sydney NSW 2000	Level 17, 201 Elizabeth Street, Sydney 2000

Version Control

Version	Effective date	Update comments	Author
1.00	1Jul00	Initial version	Governance Team
2.00	23Apr13	Update	Governance Team
2.01	2Aug13	Update	Governance Team
3.00	6Jan16	Re-written plan to incorporate audit recommendations	Governance Team
4.00	1May2022	Plan revised	Governance Team
4.01	Nov2023	Review, minor updates	PMO

Publication Information

Title	Privacy Management Plan
Document type	Plan
Policy Number	LEG2015/2
Developer	Governance Audit & Risk Management Team
Contact	Governance Audit & Risk Management Team
Approver	Commissioner
Approval date	
Effective date	
Review date	This Plan will be reviewed every three years. It will be reviewed earlier if any legislative or administrative changes affect the management of personal and health information by the NSWCC.

Annexure A: Health Records and Information Privacy Notice

The NSW Crime Commission (the Commission) has a *Sick leave policy and procedures.* The policy requires that employees provide a valid and relevant medical certificate for all leave taken in the following circumstances:

- Sick leave of more than two (2) consecutive days (days taken either side of a weekend are considered consecutive working days);
- Any sick leave taken on the working day immediately before or immediately after a public holiday;
- Any sick leave taken immediately before or after the taking of any other type of leave; and
- Any sick leave taken after notice of resignation is given;
- Any sick leave taken after a total of five (5) days of unsupported sick leave in a calendar year.

The Commission may also collect health information from employees in relation to Worker's Compensation matters.

The Health Information Privacy Principles (the HPPs), as set out in the *Health Records and Information Privacy Act 2002* (NSW) (the HRIP Act), place responsibilities on the Commission in relation to the collection and use of health information. Health information is defined in section 6 of the HRIP Act. Health information can include, among other things, a medical certificate or information about a medical appointment.

HPP 4 requires the Commission to inform employees that:

- the health information that the Commission collects will only be disclosed to your direct manager/supervisor and members of staff from the following teams:
    - payroll;
    - security; and
    - people and culture,

  for the purposes of verifying your sick leave and payment of your salary, unless you consent to disclosure to additional individuals for other purposes.
- You may request access to the health information that the Commission has collected from you.
- If you believe that the information contained in a medical certificate intrudes too much on your personal affairs, you may provide a copy of the medical certificate with redactions of any sensitive information.
- If you fail to provide the Commission with sufficient evidence of your illness in accordance with the above, such a failure may form part of your employment record.

If you require further information, please refer to the Commission's *Privacy Management Plan* or contact the Commission's Privacy Officer.

Annexure B: Privacy Complaint Internal Review Application Form

New South Wales Crime Commission

This is an application[1] for review of conduct under: (*please choose one)*

☐ **s53 of the *Privacy and Personal Information Protection Act 1998* (PPIP Act)**
☐ **s21 of the *Health Records and Information Privacy Act 2002* (HRIP Act)**

1	Name and address of the agency[2] you are complaining about: Privacy Contact Officer New South Wales Crime Commission 453 – 463 Kent Street Sydney, NSW 2000
2	Your full name:
3	Your postal address: Telephone number: Email address:
4	If the complaint is on behalf of someone else, please provide their details: What is your relationship to this person (e.g., parent)? Is the person capable of making the complaint by himself or herself? ☐ Yes ☐ No ☐ Unsure
5	What is the specific conduct[3] you are complaining about? *(see footnote for explanation of "conduct")*
6	Please tick which of the following describes your complaint: *(you may tick more than one option)* ☐ collection of my personal or health information ☐ security or storage of my personal or health information ☐ refusal to let me access or find out about my own personal or health information ☐ accuracy of my personal or health information ☐ use of my personal or health information ☐ disclosure of my personal or health information ☐ other ☐ unsure
7	When did the conduct occur (date)? *(please be as specific as you can)*
8	When did you first become aware of this conduct (date)?
9	You need to lodge this application within six months of the date at Q.8.

	If more than six months has passed, you will need to ask for special permission to lodge a late application. Please explain why you have taken more than six months to make your complaint: *(e.g., I had other urgent priorities – list them, or while the conduct occurred more than six months ago, I only recently became aware of my privacy rights, etc.)*
10	What effect did the conduct have on you?
11	What effect might the conduct have on you in the future?
12	What would you like to see the NSW Crime Commission do about the conduct? *(e.g., an apology, a change in policies or practices, your expenses paid, damages paid to you, training for staff, etc.)*

I understand that this form will be used by the NSW Crime Commission to process my request for an internal review. I understand that details of my application will be referred to the Privacy Commissioner in accordance with: section 54(1) of the PPIP Act; or section 21 of the HRIP Act; and that the Privacy Commissioner will be kept advised of the progress of the internal review.

Your signature: _____ Date: _____

Please send this form to the NSW Crime Commission Privacy Contact Officer as detailed at Q.1.

Keep a copy for your records.

For more information on the PPIP Act of the HRIP Act visit www.privacy.nsw.gov.au .

---

1 It is not a requirement under the PPIP Act or the HRIP Act that you complete an application form. This form is designed for your convenience only. However, you must make a written request in some form to the NSW Crime Commission for the matter to be a valid internal review.

2 The PPIP Act regulates NSW state government departments, area health services, most other state government bodies, and NSW local councils. Each of these is defined as a "public sector agency". The HRIP Act regulates private and public sector agencies and private sector persons.

3 "Conduct" can include an action, a decision, or even inaction by the NSW Crime Commission. For example the "conduct" in your case might be a *decision* to refuse you access to your personal information, or the *action* of disclosing your personal information to another person, or the *inaction* of a failure to protect your personal information from being inappropriately accessed by someone else.