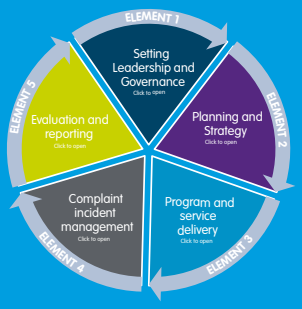
PRIVACY GOVERNANCE FRAMEWORK

Protecting and utilising personal information – a quick guide for senior executives

Enter

Diagram



ipc information and privacy commission new south wales

INTRODUCTION

Being more conscious of how to manage private personal and health information as an organisational asset will contribute to agency success and reputation.

Clever thinking about the privacy of this information, as well as compliance with legislation is essential.

NSW privacy legislation aims to achieve control by the individual of their information while meeting the needs of effective governance.

There are two privacy acts in NSW:

- the *Privacy and Personal Information Protection Act 1998* (PPIP Act), and
- the *Health Records and Information Privacy Act 2002* (HRIP Act).

Some agencies have additional privacy provisions in their legislation. If you are the head of a NSW agency, local council or university, this guide will assist you in managing privacy in your organisation by setting out the elements of a robust privacy governance framework for you to apply.

Privacy Governance Framework: contributing to agency outcomes

Hover your mouse over the elements in the diagram below to see a list of relevant privacy resources. Click on the elements to access the privacy resources to assist in embedding good privacy practices into your organisation's processes. For optimal viewing on your PC use Internet Explorer Version 9 or download to your desktop.

Proactive management of personal information, health information and privacy will add value to your agency

- Does your leadership team understand their responsibilities under privacy?
- Do your strategic objectives call for greater sharing of personal and health information with other agencies?
- Will your planned activities change the handling of personal and health information?
- Is customer trust a critical success factor for your agency, or are you keen to avoid the reputation risk if privacy complaints or data breaches are mishandled?
- Do you want to analyse data about citizen interactions, or create health records linkages to plan or improve individual/wider agency services or develop policy?
- Do you need to guarantee anonymity in data collected?
- Do you report on the management of privacy responsibilities and complaints by your agency?

The elements set out in this guide will help add value to your strategies and operations and contribute to achieving your agency outcomes.

What are the legislative essentials?

The objectives of the PPIP Act and the HRIP Act is to give individuals confidence that the handling of their personal information and health records by NSW public sector agencies is appropriate in all circumstances. Both Acts set the rules to support this.

Personal information is any information that identifies an individual such as written records which may include an individual's name and address, photographs, images, video or audio footage.

Health information is any personal information or opinion about an individual's physical or mental health; health services provided to an individual or to be provided in the future; information collected in connection with organ donation; or other personal information that is genetic information about an individual arising from a health service provided.

The PPIP Act and the HRIP Act outline the responsibilities of agencies, the rights of individuals, and the role and functions of the Privacy Commissioner. At the heart of these are the Information Protection Principles (IPPs) and the Health Privacy Principles (HPPs). They follow the 'information life cycle' as agencies collect personal and health related information, process, store and share or dispose of it. The IPPs and HPPs are complemented by other mechanisms including codes of practice (where applicable), privacy management plans and complaints management.

Agencies must comply with these core requirements. The privacy management plan should reflect the privacy governance framework within the agency. It explains how the agency will implement the IPPs and HPPs and manage their privacy obligations.

Agencies must submit their plans to the Privacy Commissioner.

Individuals have the right to see and correct their personal and health information. Individuals aggrieved by an agency's conduct can also seek an internal review from that agency or make a complaint to the Privacy Commissioner.

Agencies are required to notify the Privacy Commissioner of an internal review.

Under the PPIP Act and the HRIP Act the Privacy Commissioner may investigate and conciliate a complaint, or initiate an 'own motion' investigation, into privacy related matters. The Privacy Commissioner also monitors and reports on the PPIP Act's operation as part of her oversight role.

Further information about the PPIP Act and the HRIP Act is available from the Privacy Commissioner's website, for example see 'A guide to privacy laws' fact sheet.

What are the oversight and accountability mechanisms?

The PPIP Act and the HRIP Act make public sector agencies accountable for the way they handle personal information and health information and records, including sharing information with a third party.

These mechanisms include:

- The Privacy Commissioner's oversight role
- Parliamentary oversight of the Privacy Commissioner via the Joint Committee on the Ombudsman, the Police Integrity Commission and the Crime Commission
- The NSW Civil and Administrative Tribunal who provide individuals with a channel for review and potential redress if their privacy concerns are unresolved.

Further mechanisms available under the HRIP Act include the ability to refer complaints, where appropriate, to the Health Care Complaints Commission and the Commonwealth Privacy Commissioner.

Need flexibility?

The PPIP Act and the HRIP Act have built in flexibility and with up-front planning most activities will be possible under the two legislative regimes.

The IPPs and HPPs set general standards and can accommodate most agency circumstances and risks. In special circumstances, agencies may also develop a privacy code (which must be approved by the Attorney-General or Minister for Health, in consultation with the Privacy Commissioner), or seek a public interest direction (which modifies and/or exempts the application of the IPPs and/or HPPs and is made by the Privacy Commissioner, in consultation with either the the Attorney-General or the Minister for Health).

Agencies should approach the Privacy Commissioner in these circumstances when it is perceived that a privacy code or public interest direction may be required by the agency.

The Privacy Commissioner encourages agencies to conduct a privacy impact assessment to assist them in these circumstances.

Effective implementation of the PPIP Act and HRIP Act – making privacy an asset

An effective privacy governance framework benefits everyone and begins with leadership by the agency head.

The framework helps to clarify each person's role in privacy management and ensures that they are held to account.

Once appropriate and adequate policies, processes, systems and reporting are in place, privacy management will be a seamless integration into business-as-usual practices. This will help foster a culture of viewing privacy as an asset and not as a liability amongst your staff.

Putting it all together

Public and private sector organisations are becoming increasingly scrutinised on their handling of privacy issues and risks. Therefore, it is important to ensure that an effective privacy governance framework is in place in your agency.

Ask yourself:

- Do roles in my agency have clearly articulated privacy management responsibilities? Are the people in the role aware of their own individual accountabilities? Privacy is everybody's business.
- Do I have a forum where I can discuss privacy management issues and risks pertaining to my agency? This is because you are ultimately responsible for ensuring privacy is adequately managed in your agency.
- Does my agency have any mechanisms in place to detect when privacy breaches occur? For example, an internal incident management framework for staff to report privacy breaches at the time of occurrence. This would allow appropriate actions be taken to remediate the breach.
- Does my agency have any mechanisms in place to prevent a privacy breach from occurring? For example, IT security safeguards preventing inadvertent disclosure.
- Are my agency's privacy management plans, policy and procedures adequate and kept up to date?
- Is privacy considered as part of the agency's change management framework?

Start taking these steps to ensure that privacy is adequately managed for the benefit of your agency and the people of NSW.

Other roles and responsibilities in your agency

While the mix of roles and responsibilities will vary depending on an agency's size and circumstances, effective privacy implementation includes the following key functions and roles:

Audit and Risk Committee and security experts identify and monitor privacy breaches, agency learnings, and ensure risk frameworks adequately consider privacy risk impacts.

Privacy Contact Officers are responsible for developing privacy management plans, procedures, and conducting internal reviews. They should be sufficiently expert to inform agency staff and members of the public of privacy issues.

Managers are responsible for considering privacy issues, implementing privacy policies and procedures and managing the handling of personal information across their business unit activities (projects, programs and service delivery).

Front line staff comply with the policies and procedures set out by their agency.

The agency's Human Resources function is responsible for inducting and training staff about the agency's privacy policies and procedures.

The agency's Governance and Legal functions are responsible for ensuring and managing legal compliance, reporting and providing advice about the agency's privacy obligations and needs for flexibility.

Other legislation

There are a number of legislative instruments that contain specific exemptions to the PPIP Act and the HRIP Act, including, but not limited to:

- *Biosecurity Act 2015*
- *Cemeteries and Crematoria Act 2013*
- *Child Protection (International Measures) Act 2006*
- *Child Protection (Offenders Registration) Act 2000*
- *Children and Young Persons (Care and Protection) Act 1998*
- *Court Information Act 2010*
- *Crimes (Administration of Sentences) Act 1999*
- *Crimes (Domestic and Personal Violence) Act 2007*
- *Criminal Records Act 1991*
- *Education Act 1990*
- *Fines Act 1996*
- *Fisheries Management Act 1994*
- *Food Act 2003*
- *Government Sector Employment Act 2013*
- *Guardianship Act 1987*
- *Home Building Act 1989*
- *Housing Act 2001*
- *Independent Commission Against Corruption Act 1988*
- *Ombudsman Act 1974*
- *Parliamentary Electorates and Elections Act 1912*
- *Pesticides Act 1999*
- *Plumbing and Drainage Act 2011*
- *Police Integrity Commission Act 1996*
- *Police Regulation (Superannuation) Act 1906*
- *Radiation Control Act 1990*
- *Service NSW (One-stop Access to Government Services) Act 2013*
- *Superannuation Act 1916*
- *Workers Compensation Act 1987*

PRIVACY GOVERNANCE FRAMEWORK

information and privacy commission
new south wales