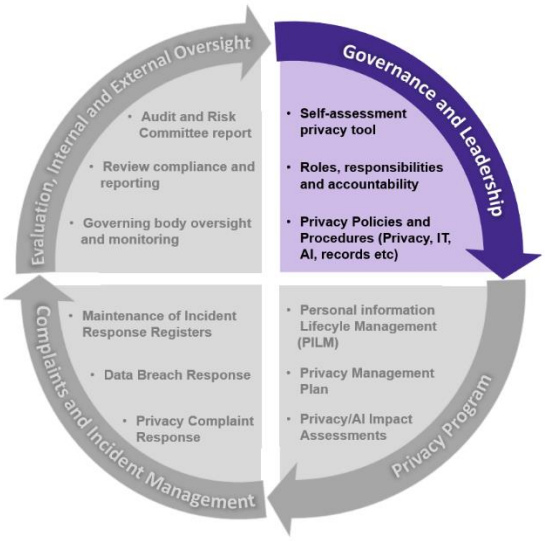
information and privacy commission new south wales

Privacy Governance Framework

February 2024

Governance and leadership



Proactive governance leadership and management of personal information, health information and privacy will improve the overall information assets of your agency and build trust with your customers and users. Public and private sector organisations are becoming increasingly scrutinised on their handling of privacy issues, information security and risks. Therefore, it is important to ensure that an effective privacy governance framework is in place in your agency.

An effective privacy governance framework benefits everyone and begins with leadership by the agency head. A 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 and personal information as an asset and not as a liability.

A privacy governance framework should be included in the agency's Privacy Management Plan.

Roles and responsibilities

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:

- **Privacy 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.
- **Information Technology** and **Cybersecurity staff** identifying and monitoring data privacy breaches.
- **Business 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).
- **Human Resources** and/or the **Training and Development** function is responsible for inducting and training staff about the agency's privacy policies and procedures.
- **Front line staff** comply with the policies and procedures set out by their agency.
- **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.
- **Audit and Risk Committees** identify and monitor agency learnings and ensure risk frameworks adequately consider privacy risk impacts.

For an agency to achieve a robust privacy program, collaboration is essential across staff with key roles and responsibilities for privacy, information security, records and other areas appropriate to that agency.

Checklist

- Does the agency's leadership team understand their responsibilities under privacy legislation?

- Is a collaborative culture evident from the interactions of those with key roles and responsibilities across the agency?
  If not, what are the steps and mechanisms that can be put in place to achieve improved interaction and collaboration to achieve a robust privacy program?
- Do roles in my agency have clearly articulated privacy management responsibilities? Are staff aware of their own individual accountabilities? Privacy is everybody's business and responsibility.
- Do I have a forum where I can discuss privacy management issues and risks pertaining to my agency?
- Does my agency have adequate mechanisms in place to detect when privacy breaches occur? For example, do the data breach policy and the internal incident management framework enable staff to report privacy breaches at the time of occurrence? Does this process facilitate appropriate actions being taken to remediate a breach?
- Does my agency have any mechanisms in place to prevent a privacy breach from occurring? For example, IT security safeguards preventing inadvertent disclosure of information.
- Are my agency's privacy management plans, policies and procedures adequate and kept up to date?
- Does the agency's privacy management plan include details about its data breach response processes?
- Is privacy considered as part of the agency's change management framework?
- Do your strategic objectives call for greater sharing of personal and health information with other agencies?
- 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?

Where to start?

Carry out a Privacy Maturity Assessment to assess your agency's systems and policies to ensure their compliance with privacy requirements – download the Privacy Self-assessment Tool.

Resources

- Fact Sheet – The PPIP Act: Agency systems, policies and practices
- Information Governance Agency Self-assessment Tools
- Agency Privacy Management Plans
- Essential Guidance Toolkit on information access and privacy fundamentals
- The PPIP Act 1998
- The PPIP Regulation 2019
- Information Protection Principles (IPPs)
- The HRIP Act 2002
- Health Privacy Principles (HPPs)
- Privacy and health records – Codes of Practice
- Privacy and health records – Public Interest Directions
- Privacy and health records – Statutory Guidelines
- Understanding your privacy obligations