Chapter 1: Key steps to embedding privacy in your health practice

Contents

Key points

- The *Privacy Act 1988* (Privacy Act) requires you to be proactive in establishing, implementing and maintaining privacy processes in your practice.
- To meet your privacy obligations and to make managing privacy easier, the key practical steps you should take are:

  Develop and implement a privacy management plan

  Develop clear lines of accountability for privacy management

  Create a documented record of the types of personal information you handle

  Understand your privacy obligations and implement processes to meet those obligations

  Hold staff training sessions on privacy obligations

  Create a privacy policy

  Protect the information you hold

  Develop a data breach response plan.

Eight key steps

The Privacy Act requires you to be proactive in establishing, implementing and maintaining privacy processes in your practice.

There are eight key steps you should take which will help you to meet this requirement. This chapter outlines the key steps you should take and provides details and links to further information.

Taking these key steps will help you to meet your privacy obligations, and make it easier to manage privacy within your health practice.

Step 1: Develop and implement a privacy management plan

The Privacy Act requires you to be proactive in establishing, implementing and maintaining privacy processes that ensure you comply with the Australian Privacy Principles (APPs).

The OAIC has developed a Privacy management framework that sets out the four broad steps you are expected to take to meet your obligations:

1. Embed: a culture of privacy that enables compliance
2. Establish: robust and effective privacy processes
3. Evaluate: your privacy processes to ensure continued effectiveness
4. Enhance: your response to privacy issues.

A key tool for meeting your obligations is to develop and implement a 'privacy management plan' that aligns your practice's business processes with your privacy obligations. A privacy management plan is a document that identifies specific and measurable privacy goals and targets to help you implement these four steps.

For more information, see the OAIC's Privacy management plan template, which is designed to help you develop a privacy management plan.

Step 2: Develop clear lines of accountability for privacy management

Your practice should have clear lines of accountability for managing privacy issues.

Knowing whom in the practice has the expertise and responsibility for meeting privacy requirements helps all staff respond efficiently to any privacy issues and seek prompt guidance when they need it.

For example, if the practice manager is responsible for privacy management, this should be clearly communicated to all staff and the practice manager should be accessible to answer any queries or to assist staff to better understand how the practice manages privacy.

Alternatively, in a larger healthcare practice — such as a private hospital — a number of staff members with particular expertise in privacy or, more broadly, regulatory requirements, might be designated privacy officers. These privacy officers can act as centralised points of contact for other staff to approach in the event that:

- they have any questions or require advice about how to handle personal information and related compliance obligations
- they need assistance in responding to a privacy-related complaint or query from a patient
- a privacy incident occurs, such as a data breach, which needs to be addressed promptly.

Step 3: Create a documented record of the types of personal information you handle

Understanding your practice's personal information holdings is an important foundation for effective privacy management and compliance.

Understanding the personal information holdings means understanding:

- **types of personal information handled**: examples include clinical notes, general patient information including contact information and Medicare/healthcare fund details, specialist reports, test results, imaging films, referral letters
- **how personal information is received**: examples include records generated within your practice, and written and verbal information from patients, other healthcare providers, insurers and lawyers
- **where personal information is held**: consider all physical and electronic records within your control, including at your premises, off-site physical locations, and cloud storage providers.

Having a thorough and documented record of the personal information you handle will help you to:

- develop a privacy policy (which must include the personal information you collect and hold)
- consider how best to protect and secure that information
- confidently and efficiently provide individuals with access to their personal information
- assess the purposes for which you can use or disclose the information consistently with your privacy obligations.

Step 4: Understand your privacy obligations and implement processes

It is important to gain an understanding of your privacy obligations.

While Chapter 1 outlines the key practical steps you should take to embed good privacy governance in your practice, the remaining chapters of this guide look in more detail at how key APPs apply to and operate in a healthcare context.

Once you understand your privacy obligations, you should develop and implement processes that facilitate your practice's compliance with those obligations.

These processes should:

- address the handling of information throughout the information life cycle — that is, consider the handling from collection, through various uses and disclosure of the information, to storage and security, and to when the information is no longer required
- clearly outline how staff are expected to handle personal information in their everyday roles

- include processes to allow individuals to easily access and correct their personal information
- include processes for receiving and responding to patients' privacy enquires and complaints.

Step 5: Staff training

Training staff on their privacy obligations and the importance of privacy will help to create a confident team that is able to handle personal information in a privacy enhancing way.

Examples of activities that can facilitate a privacy-aware culture within your practice include:

- running training for all new staff that includes information on privacy requirements and the practice's current privacy practices and expectations
- developing clear and consistent processes for staff to follow to ensure everyone is aware of their obligations and who to ask for assistance
- making privacy-related resources accessible to staff via email or, for example, by posting them on a staff intranet
- holding information sessions on emerging privacy issues or risks, developments that impact how personal information is handled, or privacy breaches or complaints that have occurred
- encouraging and facilitating professional development opportunities for staff whose role needs a deeper understanding of privacy or security.

Step 6: Create an APP privacy policy

The Privacy Act requires you to have a clearly expressed and up-to-date privacy policy which describes how you manage personal information.

Your privacy policy must cover:

- the kinds of personal information you collect and hold
- how you collect and hold personal information
- the purposes for which you collect, hold, use and disclose personal information
- how an individual may access personal information and seek its correction
- how an individual may complain if you breach the Privacy Act and how the complaint will be handled
- whether you are likely to disclose personal information to overseas recipients, and if so, the countries in which such recipients are likely to be located.

You must take reasonable steps to make the privacy policy available free of charge and in an appropriate format. This might include making the policy available on your website, or prominently displaying a copy of the policy (or instructions for how to obtain it) in your practice. If a patient asks for the policy in a particular format, you should give the individual the policy in that format.

For further information and assistance in developing a privacy policy, see the OAIC's Guide to developing an APP privacy policy and Chapter 1 of the APP Guidelines.

Step 7: Take reasonable steps to protect and secure personal information

The Privacy Act requires you to take reasonable steps to:

- protect the personal information you hold from misuse, interference, loss, and from unauthorised access, modification or disclosure
- destroy or de-identify personal information you hold once it is no longer needed.

Reasonable steps should include, where relevant, taking steps and implementing strategies in relation to the following:

- governance, culture and training
- internal practices, procedures and systems
- ICT security
- access security
- third party providers (including cloud computing)
- data breaches
- physical security
- destruction and de-identification
- standards.

For further information, see the OAIC's Guide to securing personal information.

Step 8: Develop a data breach response plan

Developing a data breach response plan is another reasonable step you can take to protect and secure personal information you hold.

A data breach is when personal information is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference. Examples of a data breach are when:

- a device containing personal information of clients is lost or stolen
- an entity's database containing personal information is hacked
- an entity mistakenly provides personal information to the wrong person.

A data breach response plan is a tool to help you manage a data breach. It is a framework setting out how you will manage and respond to a data breach, including the steps you will take and the roles of various staff members. Having a data breach response plan enables you to act quickly and effectively in the event a breach occurs.

To assist you in developing a data breach response plan, the OAIC has developed a guide to preparing a data breach response plan.

Your data breach response plan should also address notification obligations:

- You will need to notify the Australian Information Commissioner and affected individuals in the case of a breach involving personal information that is likely to result in serious harm to any affected individual.

- You will need to notify the Information Commissioner and the System Operator in the case of breaches of information held in the My Health Record system.

For further information on your data breach notification obligations, see the OAIC's Notifiable Data Breaches webpage and the OAIC's Guide to mandatory data breach notification in the My Health Record system.