



Privacy action plan for your health practice

The *Privacy Act 1988* (Privacy Act) requires you to be proactive in establishing, implementing and maintaining privacy processes in your practice.

The Office of the Australian Information Commissioner's *Guide to health privacy* sets out the key practical steps you should take to meet your privacy obligations and protect the personal information you hold:

 Develop a privacy management plan	STEP 1	Develop and implement a privacy management plan <p>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).</p>
 Be accountable	STEP 2	Develop clear lines of accountability for privacy management <p>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.</p>
 Keep records	STEP 3	Create a documented record of the types of personal information you handle <p>Understanding your practice's personal information holdings is an important foundation for effective privacy management and compliance.</p>
 Understand obligations	STEP 4	Understand your privacy obligations and implement processes to meet them <p>It is important to understand your privacy obligations and how key APPs apply to and operate in a healthcare context. Develop and implement processes that facilitate your practice's compliance with those obligations.</p>
 Train staff	STEP 5	Hold staff training sessions on privacy obligations <p>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.</p>
 Create a privacy policy	STEP 6	Create a privacy policy <p>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.</p>
 Protect personal information	STEP 7	Protect the information you hold <p>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.</p>
 Plan for a data breach	STEP 8	Develop a data breach response plan <p>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.</p>

For more information visit: oaic.gov.au/guide-to-health-privacy