Privacy and Confidentiality

mhcc.org.au

mhcc
mental health coordinating council

Privacy

Given the sensitive nature of information that people may disclose to mental health practitioners or support workers, strong privacy protection is critical to maintaining a person's trust in an organisation and the individual staff member.

Privacy legislation is designed to protect consumers from having their personal and health information exposed, either intentionally or unintentionally. Every community-managed organisation should have clear policies, procedures and risk management protocols in place to ensure the security of consumer information. These protocols should be reviewed and amended, every time a different kind of service is designed and delivered.

In the *Privacy Act 1988* (Cth), the Australian Privacy Principles govern the rights, obligations, and standards in relation to privacy. The 'Principles' govern the collection use and disclosure of personal information, governance and accountability.

Community managed organisations must comply with the 'Principles' if they:

- have annual turnover of over $3 million
- agree to comply with privacy laws in contractual arrangements with the Commonwealth government; and/or
- provides a health service to a person (even if the organisation's primary activity is not providing that health service).

In NSW, organisations that collect, hold or use health information must also comply with *Health Records and Information Privacy Act 2002* (NSW). Your organisations may still hold health information about consumers even if it does not provide a health service.

Health information includes notes of a consumer's symptoms or diagnosis, information about a health service they have had or will receive, specialist reports and test results, prescriptions and other pharmaceutical purchases, dental records, their wishes about future health services or appointment and billing details.

Digital service delivery adds a layer of complexity to protecting privacy. Digital systems can increase opportunities for consumer information to be intercepted. Reasonable steps must be taken to ensure security measures are in place that protect and control access to consumer data from misuse, interference, loss, unauthorised access, modification and/or disclosure. Consumers' personal information (including any video/audio recordings or still images) must be collected, stored, used, securely backed up and disposed of securely.

Community-managed organisations must also have processes in place to notify the Office of the Information Commissioner in the case of a notifiable data breach.

Organisations providing services to interstate consumers must comply with the privacy laws in the jurisdiction where the service is being received. For instance, if a mental health support worker in New South Wales calls a consumer while they are travelling in Victoria, they must comply with the privacy and health records laws in Victoria, as well as the *Privacy Act 1988* (Cth).

Before providing interstate services, your organisation should have an understanding of any privacy laws and other legal requirements in the jurisdictions in which you may be providing services. You may need to seek legal advice to clarify cross-jurisdictional responsibilities.

Checklist: Privacy and confidentiality

Does your organisation:

- ☐ Have a privacy policy that is compliant with the Australian Privacy Principles?
- ☐ Have a privacy policy that is compliant with Health Records and Information Privacy Act 2002 (NSW)? Are you compliant with other state laws when delivering services in that jurisdiction?
- ☐ Have a Data Breach Action Plan, including in relation to My Health Record data?
- ☐ Check compliance with privacy obligations when handling individual healthcare identifiers?
- ☐ Protect security of data transmission? For example, a secure internet service is used for digital service delivery or to transmit information, through end-to-end encryption or use of a Virtual Private Network. Documents containing personal information are encrypted, particularly when those documents are being sent by email.
- ☐ Protect security of access? For example, user authentication (password or other form of ID) for local area networks and video conferencing platforms.
- ☐ Protect security of data storage? For example, appropriate storage of all reports provided for, or generated from, the telehealth consultation.
- ☐ Conduct a Privacy Impact Assessment for each service in accordance with best practice?
- ☐ Have privacy policies for each service that:
  - are easy to understand and are transparent for consumers, their carers and supporters
  - uphold consumers' rights and choices
  - are readily available to consumers and their supporters, before accessing and while using the services; and
  - are compliant with privacy laws, privacy principles and best practice?
- ☐ Advise consumers, and where relevant, their supporters, of changes to privacy policies in a timely and comprehensible way?
- ☐ Deal with complaints in relation to an individual's data in the event of a breach?
- ☐ Have policy and procedures to educate and work with staff around privacy and confidentiality as well as data breaches?

Privacy versus Confidentiality

The concepts of 'privacy' and 'confidentiality' are related, but not the same. Privacy is a broader concept, referring to a person's right to control access their personal information and to themselves. Privacy laws regulate the handling of personal information about individuals. Privacy is a right protected by the *Privacy Act 1981* (Cth) and in the Australian Privacy Principles. Each State and Territory has its own legislation in relation to privacy obligations of its government departments and agencies.

Confidentiality ensures people or entities protect another person's or entity's information, which has been conveyed in confidence and which is not readily available to the public.

For example, health professionals have an obligation to protect the information discussed in confidence between themselves and a patient or consumer. There is no specific confidentiality legislation in Australia. However, you may have a legal duty to maintain confidentiality if you are providing a service under an agreement containing confidentiality obligation or the information is considered personal information or health information under the law.

You should ensure that confidentiality is maintained in digital service delivery to the same standard as in person service delivery.

Insurance

Your organisation's current insurance policy may or may not cover digital service delivery. It depends on the terms of your specific policy. The extent to which your digital services are similar to existing services is relevant. You should notify your insurer, preferably before you start delivering digital services and check whether these services are covered by your existing policy. You should also encourage allied health workers to check their own professional indemnity insurance.

Further resources

- The Office of the Australian Information Commissioner (OAIC) Guide to Securing Personal Information provides a useful list of relevant questions for understanding what reasonable steps you may need to take to ensure the security of personal information
  - The OIAC also has information about Privacy for health service providers.
- The Information and Privacy Commission NSW is an independent statutory authority that administers legislation dealing with privacy and access to government held information in New South Wales. The NSW Privacy Laws page has helpful information.
- The Department of Health Privacy Checklist for Telehealth Services: this checklist helps organisations to comply with privacy obligations when delivering telehealth services.
- Justice Connect Privacy page has legal information for community organisations.