ACTION GUIDE – FOR DIGITAL MENTAL HEALTH SERVICE PROVIDERS

Clinical and Technical Governance Standard:

Privacy

It is essential to ensure that all information collected by a digital mental health service remains private and secure. A privacy breach can cause serious harm to service users, including significant personal distress. Service users have a right to know that a provider has considered the privacy impacts of any information they are collecting and storing, the sensitivity of the information and how the personal information will be handled.

Privacy is protected by the *Privacy Act 1988* which outlines the Australian privacy principles (APP) for protecting personal information and the action to be taken if there is a data breach in an organisation. The Office of the Australian Information Commissioner (OAIC) is responsible for promoting and upholding the privacy rights of Australians via the Privacy Act.

All entities covered by the Privacy Act are required to have a privacy policy which includes:

- The kinds of personal information collected and stored
- How the information is collected and where it is stored
- Why the personal information is being collected
- How the information will be used and disclosed
- How someone can access their personal information or ask for it be corrected.

ACTIONS IN THE NSQDMH STANDARDS

Privacy is safeguarded via a number of actions in the National Safety and Quality Digital Mental Health (NSQDMH) Standards, as part of the Clinical and Technical Governance Standard. The relevant actions are:

- **Actions 1.16** and **1.17**, concerning the safety and security of healthcare records
- **Action 1.28**, conducting a Privacy Impact Assessment (PIA)
- **Action 1.29**, ensuring service providers have privacy policies in place
- **Action 1.30**, requiring providers to advise users when a privacy policy has changed
- **Action 1.31**, ensuring service providers have appropriate systems in place to manage data and that the use of data is transparent to service users.

Action 1.35 is also important – this requires providers to ensure they have an information security management system in place that protects the security and stability of the service.

> **Top tip:** *For guidance on how to write a privacy policy see the OAIC's Guide to developing an APP privacy policy.*

ACTION GUIDE – FOR DIGITAL MENTAL HEALTH SERVICE PROVIDERS

WHAT IS PERSONAL INFORMATION?

The Privacy Act has strict rules about how a health service provider can collect, use and disclose personal information. Personal information is:

- Information about a person's private or family life including their name, signature, and contact details
- Information about a person's working habits and practices, including their work address and contact details
- Commentary or opinion about a person.

WHAT IS HEALTH INFORMATION?

Health information is any personal information about a person's health or disability.

Some examples of health information include:

- Notes about symptoms or diagnosis
- Information about a health service a person has had or will receive
- Specialist reports and test results
- Prescriptions and other pharmaceutical purchases
- A person's wishes about future health services
- Appointment and billing details
- Any other personal information about an individual when a health service provider collects it.

Health information is commonly regarded as one of the most sensitive types of personal information. Generally consent is required before a person's health information is collected. You can find further information about the privacy obligations of health service providers in the OAIC's Guide to health privacy.

> ***'Privacy is extremely important. I think society at large is asleep at the wheel on privacy issues.'***
>
> Dr Mike Millard, Clinical Director, This Way Up

WHAT IS A PRIVACY IMPACT ASSESSMENT?

A privacy impact assessment (or PIA) is a tool for identifying and assessing privacy risks throughout the development lifecycle of a program or system. It should involve a systematic assessment to identify the impact that a digital mental health service might have on the privacy of service users, and set out recommendations for managing, minimising, or eliminating that impact. A PIA should also consider whether the planned uses of personal information in the service will be acceptable to the community.

> **Top tip:** *A 'privacy by design' approach ensures that from the outset, privacy is designed into all services that deal with personal information. Conducting a privacy impact assessment helps a service provider ensure privacy compliance and identify better practice.*

A PIA will help a service identify if their project or service delivery may lead to high privacy risks likely to have a significant impact on the privacy of individuals. This could include negative impacts on physical and mental wellbeing, reduced access to public services, discrimination, financial loss or identity theft.

The steps in a PIA process are described in the Guide to undertaking PIAs published by the OAIC. You will find other useful tools on their website including the PIA eLearning package and a template to map the types of personal information being handled by a service.

10 steps to conducting a PIA

1. Threshold assessment – do you need to undertake a full PIA?
2. Plan the PIA
3. Describe the project
4. Identify and consult with stakeholders
5. Map information flows
6. Privacy impact analysis and compliance check
7. Privacy management – addressing risks
8. Recommendations
9. Report
10. Respond and review

ACTION GUIDE – FOR DIGITAL MENTAL HEALTH SERVICE PROVIDERS

PRIVACY IMPACT ANALYSIS AND COMPLIANCE CHECK

An important aspect of a PIA is to examine the nature of privacy impacts including:

- The risk of privacy impacts on individuals (both serious and more minor) as a result of how personal information is handled
- Whether privacy impacts are necessary or avoidable
- Whether there are any existing factors that have the capacity to mitigate any negative privacy impacts
- How the privacy impacts may affect the project or service delivery's broad goals
- The effect on an individual's choices about who has access to their personal information
- Compliance with privacy law
- How the use of personal information aligns with community expectations.

PRIVACY MANAGEMENT: ADDRESSING RISKS

After analysing the privacy impacts, service providers can then consider any risks identified and how these might be mitigated. For example, are you collecting more information than is needed, using intrusive means of collection, or disclosing sensitive details more widely than is justified or necessary? Service providers should think about the ways in which they could remove, minimise or mitigate any negative privacy impacts. This will form the basis of recommendations for future practice and the PIA report. The OAIC website provides a suggested format for a PIA report together with sample PIA reports from other organisations.

> ***'It's always been a tenet of what we do to ask as little as possible about a user – only what is required to safely and effectively deliver the service.'***
>
> Dr Kylie Bennett, Managing Director, e-hub Health

PIA FOR A DIGITAL HEALTH SERVICE

The Australian Government Department of Health has published a PIA conducted for the COVIDSafe app which shows how privacy risks were assessed for this digital health service. The PIA includes recommendations such as ensuring consent is sought from users at two different points when they access the app, and ensuring a range of communication resources about privacy are available to users such as answers to frequently asked questions, summary information about the PIA report and the relevant legislation that applies.

SUMMARY: PRIVACY

Issue
Safeguarding privacy for service users

Solution
Use a range of resources available from the OAIC and other sources to write a privacy policy, undertake a PIA, and map personal information flows

Barriers
Resourcing, time commitment and financial considerations

Enablers
Executive buy-in, clear communication to staff, fostering a culture of 'privacy by design', extensive resources and templates

FIND OUT MORE

Find more information about privacy in the *NSQDMH Standards – Guide for service providers*. You can learn more about the NSQDMH Standards and other supporting resources at safetyandquality.gov.au/DMHS.

Contact the digital mental health program team at DMHS@safetyandquality.gov.au.