Australian
Commission on
Safety and Quality
in Health Care

National Safety and Quality
**Digital
Mental Health**
Standards

Fact sheet
For digital mental health service providers and accrediting agencies

Assessing cybersecurity with the Digital Mental Health Standards

Digital mental health service providers collect and use information to provide care, evaluate their services and make improvements. The systems, networks and programs that store that information are vulnerable to digital attacks and continue to be the target of malicious actors. These digital attacks represent safety issues for service users.

Digital Mental Health Standards Action 1.35 Security and stability

The service provider has information security management systems and uses a risk-based approach to:

a. Assign responsibility and accountability for information security
b. Complete and maintain an information and data inventory
c. Protect data in transit and at rest
d. Protect against interruption, damage or disconnection of the service
e. Assess the size and extent of threats to its information assets
f. Consider and mitigate vulnerabilities and threats
g. Conduct regular updates, reviews and audits of information security
h. Detect, respond and report to the governing body, workforce, service users and their support people on information security incidents and technical faults.

The Digital Mental Health Standards provide a framework for service providers to improve the quality of their services and protect service users. The following reflective questions are designed to elicit responses from service providers that support a greater understanding of the safety and quality issues related to cybersecurity:

- Have you identified all the information assets within your service and assessed the impact and likelihood of associated risks to each asset?
- Do you have a documented and regularly updated Information Security Management System aligned with a relevant industry standard (e.g. ISO 27001)? Have you applied the Essential Eight mitigation strategies and how do you assess their effectiveness?
- What procedures are in place to detect, respond to, and recover from cybersecurity incidents such as ransomware, data spills, or phishing attacks?
- How does your organisation respond to cybersecurity: have you clearly defined cybersecurity roles and responsibilities, have you appointed a Chief Information Security Officer or equivalent?
- How frequently do you assess and update your risk management framework and what criteria do you use to rate risks and plan actions related to cybersecurity?
- Can you provide evidence of staff training and ongoing professional development in cyber security awareness and incident response?
- How do you integrate advice from consultants or programs designed to improve the cybersecurity approach for the service? How do you monitor their effectiveness?

Digital mental health service providers should use a risk-based approach to address the risks and harm from the attacks on information security. Assessments may involve multiple systems that influence cybersecurity, related actions are outlined in **Table 1**.

Table 1 Digital Mental Health Standards have multiple actions related to cybersecurity

Action	Detail
Action 1.01	requires the governing body to endorse the organisation's clinical and technical governance frameworks which sets the governance and leadership of the organisation
Action 1.02	requires the organisation to use and maintain the clinical and technical governance frameworks to drive improvements in safety
Action 1.04	requires the organisation to consider the safety and quality of service users in business decision-making, for example in the development and procurement specifications
Action 1.06	requires those with technical expertise and leadership in the technical governance of the service
Action 1.07	requires the organisation to review compliance with legislation and regulation, such as those related to cybersecurity
Action 1.10	requires the organisation to plan and manage cybersecurity risks and threats
Action 1.19	requires the organisation to use its training systems to monitor the workforce's participation in training, such as those highlighting the responsibilities and procedures for information security
Action 1.23	requires the technicians involved in the design and delivery of the service has the necessary skills, experience and qualifications
Action 1.25	requires services, digital operating systems and internal access controls to be designed to maximise the safety and quality of care
Action 1.31	requires that the systems for the data of service users prevent the unauthorised re-identification of de-identified data
Action 1.36	requires the organisation to effectively manage the updates and patches of platforms and operating systems

Useful resources

- Australian Commission on Safety and Quality in Health Care (ACSHQC) \| Action guide – Information security management systems
- ACSQHC \| National Safety and Quality Digital Mental Health Standards
- Australian Signals Directorate \| Essential Eight maturity model
- Australian Signals Directorate \| Information Security Manual
- Office of the Australian Information Commissioner \| Report a data breach