ACTION GUIDE – FOR DIGITAL MENTAL HEALTH SERVICE PROVIDERS

Clinical and Technical Governance Standard:

Incident management systems and open disclosure

Despite all due care being taken, service users may sometimes be harmed as a result of accessing digital mental health services. Service providers need to prepare for how they will manage both clinical incidents and technical incidents. Clinical incidents might include a service user accessing a service that cannot adequately address the seriousness of their mental health issues. A technical incident could involve a data breach with a serious impact on the protection of privacy or a disruption to the service.

A well-designed incident management and investigation system should support the service provider and its workforce to identify, report, manage and learn from incidents. The system should comply with legislative requirements and, if relevant, with state or territory clinical incident management policies. It should be designed based on best practice guidelines set out below, and needs to be well resourced, maintained, and monitored.

ACTIONS IN THE NSQDMH STANDARDS

Incident management and investigation systems is the focus of **Action 1.11** in the National Safety and Quality Digital Mental Health (NSQDMH) Standards, as part of the Clinical and Technical Governance Standard. This action requires service providers to identify and manage clinical and technical incidents and take action to improve safety and quality.

Action 1.12 requires the service provider to use an open disclosure process to communicate with service users about unexpected poor health outcomes or harm from using its services.

This action guide describes how to establish an effective incident management system and understand the principles of open disclosure.

> **Top tip:** *The Commission provides a range of resources to inform and support service providers about the principles of open disclosure including a checklist and organisational readiness assessment tool.*

ACTION GUIDE – FOR DIGITAL MENTAL HEALTH SERVICE PROVIDERS

RISK ANALYSIS

Incident management begins with an analysis of the risks a service provider may face. The fact sheet Applying the NSQDMH Standards Using a Risk Management Approach can be used to support this process.

The following questions should be considered:

- Who is at risk?
- What is involved?
- What factors allow it to happen?
- How likely is it?
- What are the consequences?
- What can be done?
- Is there a solution for each identified situation or risk?

Service providers should also consider whether their users are particularly vulnerable groups and therefore have higher associated risks. For example, a service provider targeting young people should consider if this age group lacks other support networks and could be less likely to seek further help from a clinician if escalation of care proves necessary. A risk analysis should outline the steps to mitigate this risk.

> ***'We have a range of measures in place to ensure that the right consumers are using our tools such as the use of self-assessments that trigger prompts and pop-ups that flag to a user where this might not be the ideal intervention for them.'***
>
> Chris Rule, Manager, Quality Assurance, Service Implementation, Black Dog Institute

> **Top tip:** *The Commission's Open disclosure documentation summary template is a useful framework to help prepare for any incident discussions with service users and support people. It outlines the key points that should be covered.*

DEVELOPING AN INCIDENT MANAGEMENT POLICY

Templates and toolkits are available to help service providers develop an incident management policy. For example, the NSW Clinical Excellence Commission's website includes downloadable templates for reporting serious incidents and guidelines on complaints management. The *Best practice guide to clinical incident management* published by Queensland Department of Health may also be useful.

A risk register is a good way to consider the risks most likely to occur within a service, how to rank them in terms of their seriousness, and outline a process for managing each one. Establishing regular meetings to review safety and risk will help ensure effective ongoing monitoring.

> ***'Setting up the safety and quality technical committee ended up being a good process. Even if the numbers of people involved is small, it's still a documented responsibility and there's a meeting that has to happen on a monthly basis, and it has to report to the Board of Directors. If someone comes along and says, what incidents have you had and what have you done about them, I can point them straight to the documentation and we know exactly what's been done. That is really valuable.'***
>
> Dr Kylie Bennett, Managing Director, e-hub Health

A full incident management and investigation system should include defining what constitutes a critical incident, a technical incident or a near miss, and a framework describing the roles and responsibilities of individuals and committees, the types of events to be reported, and how to ensure confidentiality.

> ***'We scoped out everything from legal risk to clinical risk to privacy risk and then we created policies for the team. So, if there's a specific risk factor, we developed a framework to mitigate that risk.'***
>
> Dr Jonathan King, Founder and Chief Growth Officer, LYSN

ACTION GUIDE – FOR DIGITAL MENTAL HEALTH SERVICE PROVIDERS

OPEN DISCLOSURE FRAMEWORK

Adopting an open disclosure framework is an important aspect of managing incidents. Open disclosure involves a discussion between the service provider, the service user and if relevant their support people, about an incident that resulted in an unexpected outcome or harm to the service user. Open disclosure is a reasonable expectation of service users and an attribute of a high-quality service.

Open disclosure principles

- Open and timely communication
- Acknowledgement of the adverse event
- Apology or expression of regret
- Supporting and meeting the needs and expectation of patients, their family and carers
- Supporting and meeting the needs and expectations of those providing health care
- Integrated clinical risk management and systems improvement
- Good governance
- Confidentiality

Enhancing user feedback systems is vital for open disclosure to be effective. It is important to review the complaints procedure for the service and develop a register to ensure all complaints are fully considered and actioned.

SERVICE USER INPUT

There are many ways services can encourage user feedback. In addition to surveys of users, establishing a service user feedback group will be beneficial in building continuing system improvement.

> ***'There's lots of guidance around how to create incident management systems and consumer feedback systems. I'd recommend trying and testing models and then see how you can retrofit that to your organisation based on the resources you have. There's quite a bit involved in ensuring that you know how consumers interact with the organisation and that they can provide feedback.'***
>
> Chris Rule, Manager, Quality Assurance, Service Implementation, Black Dog Institute

SUMMARY: INCIDENT MANAGEMENT AND OPEN DISCLOSURE

Issue
Ensuring there is an effective system for incident management in place

Solution
Undertaking risk analysis, developing a risk framework, setting up a system of accountability to handle incidents, enhancing opportunities for users to provide feedback, incorporating an open disclosure framework

Barriers
Unclear roles and responsibilities; lack of user input

Enablers
Risk analysis process, instituting systems and frameworks, finding ways to encourage user feedback and participation

FIND OUT MORE

Find more information 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.