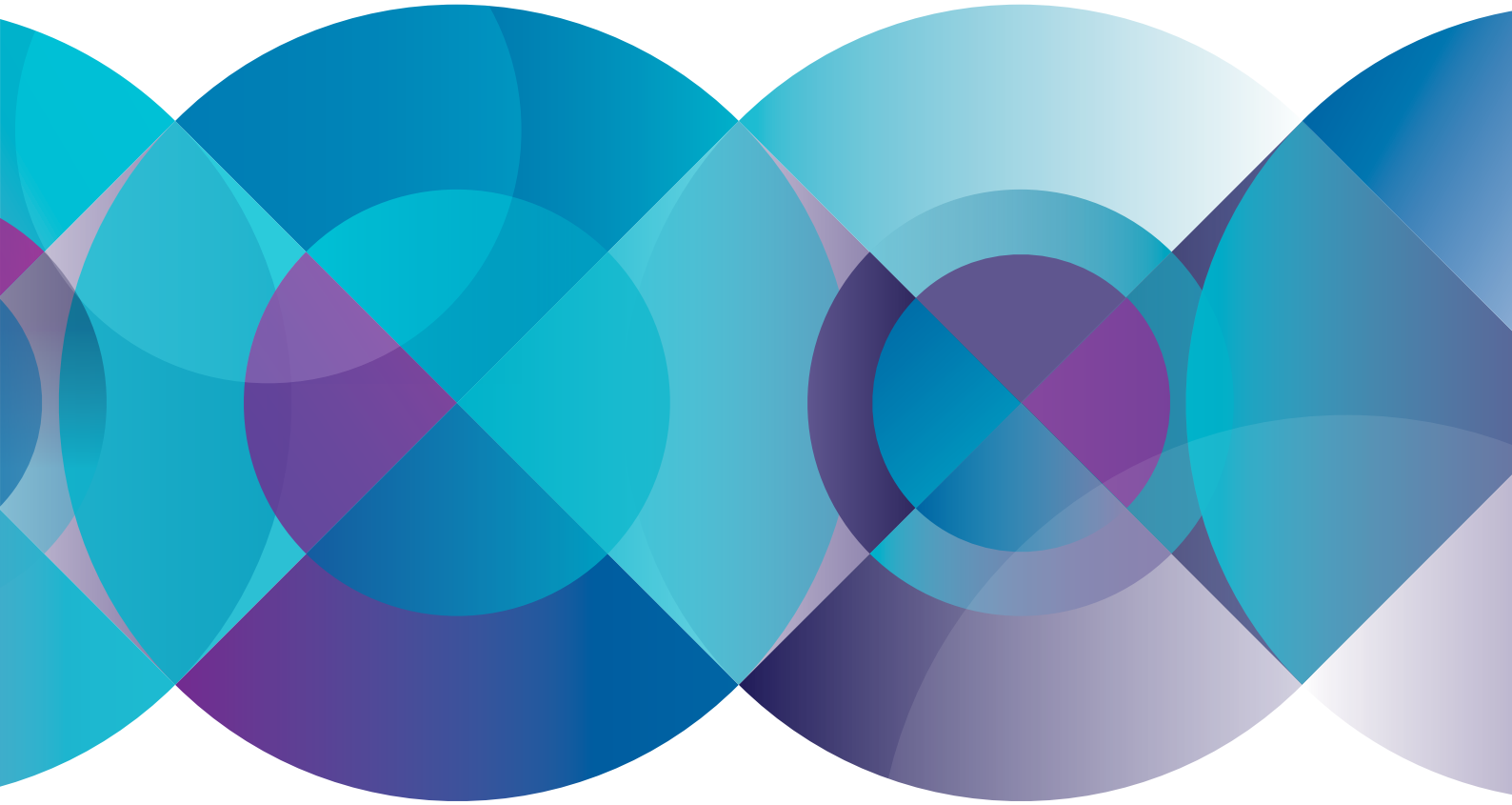
AUSTRALIAN COMMISSION
ON SAFETY AND QUALITY IN HEALTH CARE

National Safety and Quality
Digital Mental Health Standards



National Safety and Quality Digital Mental Health Standards

– Guide for service providers

February 2022

Published by the Australian Commission on Safety and Quality in Health Care

Level 5, 255 Elizabeth Street, Sydney NSW 2000

Phone: (02) 9126 3600
Email: mail@safetyandquality.gov.au
Website: www.safetyandquality.gov.au

ISBN: 978-1-922563-59-0

The Commission's preference is that you attribute this publication (and any material sourced from it) using the following citation:

Australian Commission on Safety and Quality in Health Care. National Safety and Quality Digital Mental Health Standards – Guide for service providers. Sydney; ACSQHC, 2022

Disclaimer

The content of this document is published in good faith by the Australian Commission on Safety and Quality in Health Care for information purposes. The document is not intended to provide guidance on particular healthcare choices. You should contact your healthcare provider on particular healthcare choices.

The Commission does not accept any legal liability for any injury, loss or damage incurred by the use of, or reliance on, this document.

Acknowledgement

The Commission would like to thank our partners for their contributions to the development of the *National Safety and Quality Digital Mental Health Standards – Guide for service providers* and their continuing commitment to improving safety and quality across the Australian healthcare system.

Sea urchin design: Ms Tanya Taylor is a Worimi artist (mid-north coast of New South Wales) who is drawn to the underwater world through a deep connection with her saltwater heritage. Tanya's design is inspired by the patterns found in the sea urchins, corals and sea creatures found in the ocean.

Contents

Table of Actions

Clinical and Technical Governance Standard

Model of Care Standard

Introduction

Digital mental health services offer new and innovative ways to access services, and have seen strong growth over the past decade. These services can be used as standalone supports that are self-managed or therapist-guided, or as a complement to in-person services. Digital services may be easier to access than in-person services, and sometimes can be used anonymously to protect service user identity[1], which may encourage fuller disclosure and engagement.

There is growing evidence about the important role digital mental health services can play in the delivery of services to a wide variety of consumers, carers, and families.[2] Younger people are often seen as the main users of digital mental health services, but as our population becomes increasingly familiar with digital technology, age and disability are not necessarily barriers to the use of these services. Some digital services have been evaluated and shown to be as effective as in-person services[3–5], while others have not been subject to rigorous evaluation processes or evidence collection.[6–9]

The Australian Commission on Safety and Quality in Health Care (the Commission) released the National Safety and Quality Digital Mental Health (NSQDMH) Standards[10] in November 2020. The NSQDMH Standards were developed in collaboration with consumers, carers, families, clinicians, service providers, and technical experts.

The development of the NSQDMH Standards is an important step in providing safety and quality assurance for digital mental health service users and their support people, and best-practice guidance for service providers and developers.

The NSQDMH Standards complement existing regulatory provisions that apply to digital mental health services or their providers, including consumer law, privacy and health records laws and principles, health practitioner registration, and regulation of medical devices, including software that meets the definition of a medical device.

The primary aim of the NSQDMH Standards is to improve the quality of digital mental health service, and provision and to protect service users and, where relevant, their support people from harm. The NSQDMH Standards provide a quality assurance mechanism that tests whether systems are in place to ensure that expected standards of safety and quality are met. The NSQDMH Standards provide a nationally consistent statement about the standard of care service users and their support people can expect from a digital mental health service.

What do the NSQDMH Standards cover?

There are three NSQDMH Standards, which cover clinical and technical governance, partnering with consumers, and the model of care (which includes communicating for safety and recognising and responding to acute deterioration).

The three NSQDMH Standards are:

- Clinical and Technical Governance Standard, which describes the clinical and technical governance, safety and quality systems, workforce qualifications and skills, and the safe environment (including privacy, transparency, security and stability of digital systems) that are required to maintain and improve the reliability, safety and quality of digital mental health care, and improve health outcomes for service users.
- Partnering with Consumers Standard, which describes the systems and strategies to create a person-centred digital mental health system in which service users, and where relevant their support people, receive:
  - included in shared or supported decision-making
  - partners in their own care
  - involved in the development and design of quality digital mental health care.
- Model of Care Standard, which describes the processes for establishing and delivering the model of care, minimising harm, communicating for safety, and recognising and responding to acute deterioration in mental state.

How to use this guide

The Commission has developed the National Safety and Quality Digital Mental Health Standards – Guide for service providers to assist service providers to align their clinical and technical safety and quality improvement programs with the framework of the NSQDMH Standards.

This guide should be used as a reference by service providers implementing the NSQDMH Standards. It can be used alongside other resources, including the self-assessment tool and fact sheets available at www.safetyandquality.gov.au/dmhs.

The suggested strategies, evidence and resources provided in this guide are not mandatory. Service providers can choose improvement strategies that are specific to their context. These strategies should be meaningful, useful, and relevant to the service provider's governance, structure, workforce, and service users.

This guide includes examples of the evidence service providers may use to show that they meet each of the actions in the NSQDMH Standards. Service providers vary in size and structure and will have different ways of developing and presenting evidence.

For each standard in this guide there is a:

- **Description of the standard**

> Service providers establish a model of care for each digital mental health service, and implement and maintain systems to support the delivery of safe and high-quality care and to minimise the risk of harm to service users, their support people and others.

- **Statement of intent**

> **Intention of this standard**
>
> To ensure digital mental health services have a clearly defined model of care, consistent with best practice and evidence and service users, and where relevant, their support people, receive care consistent with the model of care.

- **List of criteria that describe the key areas covered by the standard**

> **Criteria**
>
> Establishing the model of care
>
> Delivering the model of care
>
> Minimising harm
>
> Communicating for safety
>
> Recognising and responding to deterioration

- **Explanatory notes on the context of the standard**

> **Explanatory notes**
>
> **Model of care**
>
> The model of care outlines the way a digital mental health service is to be delivered. Service users and their support people access digital mental health services through many channels and media, and the model of care for their chosen services may not always be obvious.

Each action includes the following sections:

Actions

Actions with the icon shown below denote content of particular importance for Aboriginal and Torres Strait Islander peoples.

Action 3.07

The service provider has processes to:

a. Routinely ask if a service user is of Aboriginal and/or Torres Strait Islander origin, and to record this information in administrative and clinical information systems

b. Authenticate service users and match them to their care...

Intent of the action

Summarises the intended outcome of implementing the action.

Intent of the action

The service provider has a model of care for each digital mental health service that enables and supports the delivery of care to service users.

Reflective questions

Poses questions to the service provider to help them evaluate the extent to which they currently meet the action.

Reflective questions

- How does the service provider document the model of care for each service, including outlining the intended users?
- What processes are in place to monitor and evaluate whether the models of care for each service are effective?
- What actions does the service provider take to update and improve the models of care of its services?

Meeting the action

Includes key tasks for implementing the action.

Meeting the action

The model of care describes the purpose and intent of the digital mental health service and broadly defines the way the service is organised and delivered. It considers the context of the digital mental health service, and the category of service that it aims to deliver, and outlines which interventions will be provided, when, how, to whom and for what purpose.

Examples of evidence

Lists examples of evidence that a service provider could submit for an accreditation assessment. It is not expected that service providers will have examples of all the listed forms of evidence in place.

Examples of evidence

Examples of evidence may include:

Literature searches that show the evidence relied upon by the model of care at the time of development of each service

Clinical guidelines that set out best practice for the services being delivered

An audit of the alignment of the model of care for a service with the available evidence and best practice.

What is a digital mental health service?

In the NSQDMH Standards, a digital mental health service is defined as a mental health, suicide prevention or alcohol and other drug service that uses technology to facilitate engagement and the delivery of care.

This includes services providing information, digital counselling services, treatment services (including assessment, triage and referral services) and peer-to-peer support services via telephone (including mobile phone), videoconferencing, the web (including webchat), SMS or mobile health applications (apps).

When using the term **digital mental health services** to refer to all such services delivered via a digital platform, the Commission recognises the distinct specialist mental health, suicide prevention, and alcohol and other drug sectors that provide services to often-distinct cohorts.

Digital products that are not used directly to facilitate engagement or the delivery of care do not meet the definition of a digital mental health service used in the NSQDMH Standards. Standalone electronic health or medical records, decision-support tools for clinicians, analytic services, services that primarily provide support and education to health professionals, clinical practice management software, and clinical workflow and communication software are also excluded under the definition of digital mental health services used in the NSQDMH Standards.

The NSQDMH Standards are not intended to apply to telephone services used only for intake, or a single occasion of post-discharge follow-up for a service that is otherwise delivered entirely in person. However, these services may wish to be guided by the NSQDMH Standards.

The NSQDMH Standards are not intended to apply to more generic wellness services that do not offer specific health services to service users or their support people. However, providers of generic wellness services may use relevant components of the NSQDMH Standards to guide their service delivery expectations, especially in technical areas such as privacy, transparency, security, costs and advertising, usability, and accessibility. The NSQDMH Standards are voluntary, so it is up to the service provider to decide whether they wish to apply the standards to the digital services they offer.

How should the NSQDMH Standards be applied?

The NSQDMH Standards are voluntary but the benefits of implementing them include greater public trust and uptake of digital mental health services and enhanced empowerment and choice for service users.

The NSQDMH Standards should be applied at the level of service providers that make digital mental health services available to service users and their support people.

Not all actions within each standard are applicable to every digital mental health service. A service provider may provide more than one digital mental health service and the application of the NSQDMH Standards may vary across those services. If a service provider determines that certain actions within the NSQDMH Standards do not apply to one or more of the digital mental health services that they make available, they are advised to document the rationale for that determination and make it available to others if requested.

The applicability of actions and the extent of the strategies required will be determined by the size, risk to service users and their support people, and the complexity of the service provider's digital mental health services. The model of care used by the digital mental health service may also inform whether an action is relevant.

The NSQDMH Standards are intended to apply only to service providers' digital mental health services (including digital suicide prevention and alcohol and other drugs services), not to other service components.

To meet the NSQDMH Standards, service providers will need to work closely with developers of digital mental health services on the design and development of their products

and delivery of their products to service users and their support people.

The NSQDMH Standards provide a useful reference to guide the development of a digital mental health service. An assessment of a service provider's conformance to the Standards can be undertaken at any time during the lifecycle of the digital mental health service.

Who is a service provider?

Service providers may be large or very small, and may be non-government, public or private organisations or individual providers who make a digital mental health service available for others to use. How the NSQDMH Standards are met will vary between service providers, because their safety and quality systems and processes will be tailored to the context of their service.

An individual health practitioner who **recommends** the use of a digital mental health service as part of a therapeutic program is not considered to be a service provider, whereas an individual health practitioner who **provides** a digital mental health service is considered to be a service provider. For example, a psychologist who has developed an app and makes it available to consumers, carers, and families for their use is a service provider.

A service provider that has developed a digital mental health service but does not deliver the service itself is not regarded as the service provider of that service when applying the NSQDMH Standards. For example, a digital mental health service may be licensed to other service providers to deliver. In contrast, if an organisation contracts another entity to deliver a digital mental health service on its behalf, the contracting organisation is regarded as the service provider of that service for the purposes of the NSQDMH Standards.

Alignment with other standards

In developing the NSQDMH Standards, the Commission has adapted some actions and terminology from the National Safety and Quality Health Service (NSQHS) Standards (second edition).[11]

If a service provider that is required to meet the NSQHS Standards also offers digital mental health services, only the actions unique to the NSQDMH Standards are recommended for implementation in addition to the NSQHS Standards. This ensures that the issues specific to digital mental health services are given appropriate focus.

The NSQDMH Standards have been mapped to the NSQHS Standards.[12] The resulting mapping tool will assist service providers to easily understand which actions they are required to complete if they are already accredited to the NSQHS Standards.

Service providers may also hold other types of certification that relate to the digital mental health services they provide, such as the international standard ISO 27001 – Information Security Management.[13] While other certification processes do not replace the need for a service provider to examine the wide variety of clinical and technical actions within the NSQDMH Standards, they may provide evidence of conformance to the relevant actions.

A word about language

The language we use is important and must be selected wisely. It has the power to offer hope and encouragement or to convey pessimism or low expectations. It can worsen or mitigate the stigma attached to mental illness, alcohol and other drug use, and suicide.

The terminology in common use across different domains in the health sector is not universal, especially when referring to those who seek assistance from health services. The NSQDMH Standards refer to those who use digital mental health services as **service users**.

If reference is made to **consumers, carers, and families**, as opposed to service users, this is intended to specifically refer to those with lived experience, who may or may not have used digital mental health services.

Individuals who provide support and reassurance to service users are referred to as **support people** and may be family members, friends, or paid support workers.

An organisation that makes digital mental health services available to service users is referred to as a **service provider**. The services, whether they are information services, digital counselling services, treatment services (including assessment, triage and referral services), or peer-to-peer services, and irrespective of the digital medium through which they are provided, are referred to in the NSQDMH Standards as **digital mental health services**.

This terminology is adopted for clarity of purpose within the NSQDMH Standards, but service providers need not adopt the language used in the NSQDMH Standards within their own organisation.

A **glossary** is provided (see page 195) to help readers understand the terms used.

More information

For more information on the NSQDMH Standards, visit the Commission's website: www.safetyandquality.gov.au/dmhs.

Resources to assist service providers to implement the NSQDMH Standards are available on the Commission's website.

The Safety and Quality Advice Centre provides support for service providers on NSQDMH Standards implementation.

Email: advicecentre@safetyandquality.gov.au

Phone: 1800 304 056

Clinical and Technical Governance Standard

Service providers have a responsibility to the community for continuous improvement of the safety and quality of their services, and ensuring that they are person-centred, safe, and effective.

Intention of this standard

To implement a clinical and technical governance framework that ensures service users and their support people receive safe and high-quality care.

Criteria

Governance, leadership and culture

Safety and quality systems

Workforce qualifications and skills

Safe environment for the delivery of care

Explanatory notes

Delivering digital mental health services requires consideration of both clinical and technical governance to ensure safe and high-quality service delivery and service user experience.

Clinical and technical governance should be integrated components of a service provider's corporate governance. Good governance ensures that everyone – from the workforce to managers and members of governing bodies, such as boards – is accountable to service users, their support people and the community for assuring the delivery of digital mental health services that are safe, effective, integrated, high-quality and continuously improving.

Clinical governance

Thorough research has identified the elements of an effective clinical governance system and the effect of good clinical governance on health service performance.[14–16] Clinical governance is the set of relationships and responsibilities established by a service provider between its governing body, executive, workforce, service users and other stakeholders to ensure good clinical outcomes. It ensures that the service provider, service users and their support people can be confident that systems are in place to deliver safe and high-quality health care and to continuously improve services.

Leaders have an important role in influencing the quality of care by setting priorities, shaping culture, supporting the workforce, engaging effective digital mental health services, and monitoring progress in their safety and quality performance. Managers and the workforce also play an important role in clinical governance, aligning clinical and technical priorities and supporting continuous quality improvement.

The Commission has developed the National Model Clinical Governance Framework[17] to support the delivery of safe and high-quality care. Service providers should refer to the framework for more details on clinical governance, and the associated roles and responsibilities.

Technical governance

Technical governance is the system by which the use of digital information and communication technology is directed and controlled. It includes leadership, organisation structures, strategy, policies, and processes to ensure that the provider's digital technology sustains and extends the organisation's strategies and objectives.

Service providers should take a systematic approach to the governance of information management and information and communication technology. The approach should be part of their corporate governance framework.

Implementing this standard

This standard integrates actions for the clinical and technical governance of digital mental health services. Recognising the shared elements – for example, leadership, culture, incident management, and interdependencies – service providers may need to cross-reference actions between the clinical and technical workforces to minimise duplication and improve outcomes.

Each service provider should put in place strategies for clinical and technical governance that consider its own circumstances and context.

Criterion: Governance, leadership and culture

Service providers set up and use clinical and technical governance systems to improve the safety and quality of care.

Corporate governance encompasses the establishment of systems and processes that shape, enable and oversee the management of an organisation, regardless of whether the organisation is large or small. It is the activity undertaken by governing bodies (often boards but sometimes sole directors) of formulating strategy, setting policy, delegating responsibility, supervising management, and ensuring that appropriate risk management and accountability arrangements are in place throughout the organisation.

Management has an operational focus, whereas governance has a strategic focus. Managers run organisations, whereas the governing body ensures that the organisation is run well and in the right direction. It is the governing body's responsibility to ensure good governance.

Leaders, managers, clinicians, peer workers, and technicians have important roles in influencing the safety and quality of digital mental health services by shaping culture within the organisation, setting direction, providing support to the workforce, and monitoring progress and improvement in clinical and technical safety and quality performance.

The responsibility of the governing body for clinical and technical governance of digital mental health services is an integrated element of its overall responsibility and accountability for the governance of the organisation.

Clinical and technical governance relies on well-designed systems that deliver, monitor and account for the safety and quality of the care delivered to digital mental health service users. Multidisciplinary digital health safety teams that include clinicians and experts in IT systems and health informatics can aid in the governance, design, implementation and monitoring of digital mental health services.

Although it is ultimately the responsibility of a governing body to set up sound clinical and technical governance systems and be accountable for the outcomes and performance within these systems, implementation involves contributions by developers of the digital mental health services as well as individuals and teams within the organisation making the digital services available.

As part of governance, the governing body:

- Establishes the strategic direction for the digital mental health services to be provided
- Endorses a strategic and policy framework that supports digital mental health service delivery
- Delegates responsibility for operating the service provider organisation (including digital mental health services) to the chief executive officer, who in turn delegates specific responsibilities to the workforce
- Supervises the performance of the chief executive officer
- Monitors the service provider's performance, including the performance of its digital mental health services.[17]

Governance, leadership and culture

Action 1.01

The governing body:

a. Provides leadership to develop a culture of safety and quality improvement, and satisfies itself that this culture exists within the organisation

b. Provides leadership to ensure partnering with service users and their support people

c. Sets priorities and strategic directions for ethical, safe and high-quality care, and ensures that these are communicated effectively to the workforce and service users and their support people

d. Endorses the organisation's clinical and technical governance frameworks

e. Ensures that roles and responsibilities are clearly defined for the governing body, management, clinicians, peer workers, technicians, and other members of the workforce

f. Monitors the action taken as a result of analyses of clinical and technical incidents and trends

g. Reviews, reports and monitors the organisation's progress on safety, quality, performance, and effectiveness

h. Establishes principles and practices within governance frameworks that support the organisation's ability to adapt to technology as it changes.

Intent of the action

The governing body must assure itself that a culture of safety and quality improvement operates in the service, encompassing both clinical and technical components.

Reflective questions

- How does the governing body understand and promote safety and quality?
- How does the governing body observe ethical standards in the delivery of services?
- How does the governing body set strategic direction, and define safety and quality roles and responsibilities?
- What information does the governing body use to monitor progress and report on strategies for safe and high-quality clinical care?

Meeting the action

Identify the governing body

The service provider should start by identifying the governing body – this is the group of people with ultimate responsibility and accountability for decision-making about safety and quality for digital mental health services.

Define governance processes

The governing body has obligations to ensure that effective clinical and technical safety and quality systems, and robust governance processes are in place and performing well.

The governing body and management should regularly assess the systems in place to help them perform their clinical and technical governance roles.

Tasks for implementing the action:

- Determine the priorities and strategic directions for the digital mental health services to be provided
- Describe the expected outcomes in safety and quality through the organisation's vision, mission, and goals
- Identify the appropriate structures and processes to manage and monitor clinical and technical performance
- Set the requirements for time frames, targets, and reporting on clinical and technical safety and quality performance
- Incorporate changes in technology into strategic and business planning
- Monitor implementation and compliance with strategic, business, and safety and quality improvement plans
- Endorse the service provider's clinical and technical governance frameworks and the ethical principles that apply to digital mental health services
- Endorse the service provider's strategic plans (such as the safety and quality improvement plan), the information security management plan, privacy impact assessment, and the plan for partnering with service users, consumers, carers, families, and support people
- Review the organisational structure and the position descriptions and contracts for the workforce, and ensure that roles, responsibilities and accountabilities for clinical and technical safety and quality of digital mental health services are clearly defined and articulated at all levels in the organisation
- Review processes for reporting to the governing body on safety and quality indicators, and ensure that it covers all digital mental health services, major risks, clinical and technical dimensions of quality, and key elements of the quality improvement system.

When a service provider contracts the development of a digital mental health service from an external provider, the contract should clearly specify the requirements and accountabilities for clinical and technical safety and quality that the mental health service must incorporate.

When a service provider that has developed a digital mental health service licenses another service provider to deliver the service, the contract or agreement between the licensor and the licensee should clearly specify the requirements and accountabilities of each for clinical and technical safety and quality. For example, the service provider who has developed the service is responsible for ensuring that the service is based on the best available evidence and best practice, whereas the service provider who is licensed to deliver the service is responsible for how the service is delivered and the outcomes it achieves. There should be evidence of ongoing liaison between the two service providers about the safety and quality of the licensed digital mental health service.

The governing body should also consider how its focus on the governance of digital mental health services aligns with the governance of its non-digital services (if applicable), and should consider opportunities to enhance the engagement of the broader organisation with digital mental health services.

Define safety culture

Positive safety cultures in health care are driven by strong leadership that prioritises the safety of all. Commitment from leadership and management is important because their actions and attitudes influence the quality of the digital mental health services provided, as well as the perceptions, attitudes, and behaviours of members of the workforce who support the delivery of digital mental health services.

A positive safety culture is not the same as cultural safety. For Aboriginal and Torres Strait Islander peoples, cultural safety is determined by Aboriginal and Torres Strait Islander individuals, families, and communities (see Action 1.20).[18]

Tasks for implementing the action:

- Provide strong leadership to drive the safety culture
- Show management commitment to safety culture by making it a key organisational priority
- Promote a culture that encourages the safe and prompt reporting of incidents or near misses by all involved
- Educate the workforce to remain alert to the possibility that things can go wrong
- Acknowledge at all levels that mistakes occur
- Set up systems to recognise, respond to, give feedback about, and learn from, clinical and technical incidents.

Involve service users, consumers, carers, families, and support people

The governing body should promote engagement with service users, consumers, carers, families, and support people, and ensure that effective partnerships are developed.

Tasks for implementing the action:

- Ensure representation of people with diverse needs and from diverse backgrounds (see Action 2.07)
- Provide information about each digital mental health service to potential service users via the product information template (see Action 3.03)
- Specify how service users, consumers, carers, families, and support people are engaged in the governance, planning, design, measurement, and evaluation of digital mental health services
- Allocate time in meetings to hear and discuss, with respect and dignity, stories or feedback from digital mental health service users and their support people; if possible, get the service user's consent on what and how to share their experience
- Ensure that resources are available to support activities such as engaging with service users, consumers, carers, families, and support people, and collecting data on the experience of service users
- Include service users, consumers, carers, families, or support people representatives on committees and working groups.

Define service user experience

The governing body should define the expected quality of the experience for those using digital mental health services. Setting priorities and targets for safety and quality enables the organisation to define the specifications for digital mental health services to achieve these goals, and to set up systems that support quality user experiences.

Tasks for implementing the action:

- Incorporate user experience into strategic plans that are translated into operational statements, policies, procedures and protocols
- Include analysis of aggregated reports of user experience in regular and ad hoc communication to the intended audiences for the digital mental health services, and indicate how this information has been used to inform service improvement.

Define quality indicators

The governing body should regularly review quality indicators for digital mental health services to ensure that they are relevant and comprehensive.

Key indicators may include:

- Compliance with key legislative and regulatory requirements
- Compliance with evidence-based and best-practice pathways
- A selection of measures covering clinical and technical dimensions of quality such as accessibility, utilisation, privacy, data security, clinical effectiveness, user experience, efficiency, and appropriateness of care
- Trends in feedback and complaints from service users, and action taken to resolve complaints or issues
- Trends in reported clinical and technical incidents and near misses, and actions taken
- Risk ratings.

Monitor and review performance

The governing body is responsible for reviewing reports and monitoring the clinical and technical safety and quality performance of its digital mental health services, including service user outcomes.

Tasks for implementing the action:

- Agree upon the template and calendar for reporting to the governing body on safety and quality indicators and data
- Review relevant data from clinical and technical incidents and reports of complaints
- Review the organisation's audit program to ensure that it includes clinical and technical safety and quality content
- Ensure that mitigation strategies are in place to manage all major risks
- Review the processes for providing feedback to the workforce, service users and their support people, and the community about the safety and quality performance of the digital mental health services provided.

Emphasise recovery-orientated services

Recovery is defined as 'being able to create and live a meaningful and contributing life in a community of choice with or without the presence of mental health issues'.[18]

Key tasks for the governing body to support recovery for service users of digital mental health services include:

- Define expectations about the recovery focus of digital mental health services
- Set measures that ensure recovery is prioritised as part of service quality and delivery.

Examples of evidence

Examples of evidence may include:

An organisational charter or constitution

Policy documents that describe the roles and responsibilities of the governing body and the workforce

The service provider's ethical principles, and processes for partnering with service users

Strategic, business or risk management plans endorsed by the governing body that describe the priorities and strategic directions for safe and high-quality services

Codes of conduct that are endorsed by the governing body

Committee and meeting records in which clinical and technical governance, leadership, safety and quality culture, performance and effectiveness, or partnering with service users and their support people, are discussed

Documented clinical and technical governance frameworks that are endorsed by the governing body

Contracts with vendors/developers of digital mental health services that clearly define the roles and responsibilities in the governance and monitoring of digital mental health services (if applicable)

An audit framework or schedule that is endorsed by the governing body

Safety and quality performance and effectiveness data (including outcome measures), compliance reports and reports of clinical and technical incidents that are monitored by the governing body, managers or the clinical or technical governance committees

Workforce safety survey reports

Employee opinion survey reports

A cultural assessment tool used by the service provider, and reports of assessments conducted

Rainbow Tick assessment or accreditation

An annual report that includes information on the service provider's safety and quality performance and effectiveness

Terms of reference or letter of appointment to the governing body that describes members' safety and quality roles and responsibilities

Communication with the workforce or service users on the clinical and technical governance frameworks for safety and quality performance.

Useful resources

1. National Model Clinical Governance Framework. Available at: www.safetyandquality.gov.au/publications-and-resources/resource-library/national-model-clinical-governance-framework[17]
2. A National Framework for Recovery-Oriented Mental Health Services: Policy and theory. Available at: www.health.gov.au/resources/publications/a-national-framework-for-recovery-oriented-mental-health-services-policy-and-theory[19]
3. National Agreement on Closing the Gap. Available at: www.closingthegap.gov.au/national-agreement/national-agreement-closing-the-gap/3-objective-and-outcomes[20]
4. National Aboriginal and Torres Strait Islander Health Plan. Available at: www.health.gov.au/health-topics/aboriginal-and-torres-strait-islander-health/how-we-support-health/health-plan[21]

Organisational leadership

Action 1.02

The service provider establishes and maintains clinical and technical governance frameworks, and uses the processes within these frameworks to drive improvements in safety, quality, performance, and effectiveness.

Intent of the action

The service provider's clinical and technical governance frameworks are comprehensive and effective in improving clinical and technical safety and quality.

Reflective questions

- Does the service provider have documented clinical and technical governance frameworks?
- How are the clinical and technical governance frameworks integrated in practice?
- How is the effectiveness of the clinical and technical governance frameworks reviewed?

Meeting the action

Develop clinical and technical governance frameworks

As a component of broader systems for corporate governance, clinical governance involves a complex set of leadership behaviours, policies, procedures, and monitoring and improvement mechanisms that are directed towards ensuring good clinical outcomes.

Technical governance likewise involves leadership, policies, procedures, monitoring, and improvement mechanisms directed towards ensuring good technical outcomes (such as privacy, transparency, security, stability and continuity) that also support good clinical outcomes.

Although clinical and technical governance have distinct areas of focus, there will likely be overlap in the systems and processes used to deliver them, and an integrated approach should be the goal.

Tasks for implementing the action:

- Implement policies, procedures and protocols that describe the clinical and technical governance frameworks
- Include clear definitions for clinical and technical safety and quality in the frameworks, and articulate reporting lines, roles and responsibilities, and accountabilities
- Maintain cross-functional subject matter expertise, including clinical and technical skills and business management skills, to inform clinical and technical governance
- Provide and sustain the resources and focus necessary to assure the infrastructure and processes for service user safety in a digital environment
- Educate the workforce about the key aspects of the clinical and technical governance frameworks, and their responsibilities for improving clinical and technical safety and quality.

Implement clinical and technical governance systems

Service providers are responsible for implementing well-designed and integrated systems to operationalise effective and consistent clinical and technical governance systems.

Tasks for implementing the action:

- Establish one or more committees responsible for overseeing clinical and technical governance
- Review policies, procedures and protocols to ensure they align with the clinical and technical governance frameworks
- Review results of clinical and technical audits and system evaluation reports to evaluate compliance with the clinical and technical governance frameworks
- Identify and manage clinical and technical risks
- Ensure quality improvement in clinical and technical systems
- Manage models of care and clinical practice
- Manage technical performance, including privacy, transparency, security, stability and continuity
- Manage workforce performance and skills
- Manage clinical and technical incidents and complaints
- Ensure service users' rights are protected.

Monitor clinical and technical governance systems

To ensure the effectiveness of clinical and technical governance systems, service providers should use the clinical and technical governance frameworks to:

- Monitor, analyse and report on clinical and technical performance
- Collect, analyse, and report on feedback, and use this to inform quality improvement
- Recommend actions to improve the clinical and technical safety and quality of the digital mental health services and provide advice to the governing body about the issues identified and actions taken
- Review the implementation of the clinical and technical governance frameworks.

Examples of evidence

Examples of evidence may include:

Documented clinical and technical governance frameworks

Documented safety and quality goals and performance and effectiveness indicators for the services provided by the service provider

A documented organisational and committee structure that is aligned to the clinical and technical governance frameworks

Audit results showing compliance with the service provider's clinical and technical governance frameworks, and management of safety and quality risks

Reviews or evaluation reports on the effectiveness of the service provider's safety and quality systems for services.

Useful resources

1. National Model Clinical Governance Framework. Available at: www.safetyandquality.gov.au/publications-and-resources/resource-library/national-model-clinical-governance-framework[17]

Action 1.03

The service provider implements and monitors strategies to meet its priorities for diverse population groups, including Aboriginal and Torres Strait Islander peoples, and inclusion of service users and, where relevant, their support people.

Intent of the action

The health needs of diverse population groups, including Aboriginal and Torres Strait Islander peoples, are identified, and strategies are implemented to improve the safety and quality of care provided.

Reflective questions

- How are the needs and priorities of diverse population groups considered and identified?
- What are the community-defined needs of Aboriginal and Torres Strait Islander peoples?
- What strategies are used to improve outcomes for diverse population groups using the services?
- How are these strategies monitored, evaluated, and reported?

Meeting the action

Setting priorities for Aboriginal and Torres Strait Islander service users

The two compelling reasons to have specific actions that meet the needs of Aboriginal and Torres Strait Islander peoples are:

- The historical and contemporary context of Aboriginal and Torres Strait Islander health
- The unique and diverse cultures of Aboriginal and Torres Strait Islander peoples.[22]

The NSQHS Standards User Guide for Aboriginal and Torres Strait Islander Health may assist service providers to interpret and apply the actions in the NSQDMH Standards that refer specifically to Aboriginal and Torres Strait Islander peoples.

Meaningful, lasting relationships with the Aboriginal and Torres Strait Islander community are integral to redressing past wrongs and moving towards an equitable healthcare system for all Australians.

Tasks for implementing the action:

- Review the membership of the governing body to ensure inclusion of Aboriginal and Torres Strait Islander peoples
- Form sustainable relationships with Aboriginal and Torres Strait Islander peoples and inform service delivery as a result of the input of Aboriginal and Torres Strait Islander people
- Work with relevant communities to understand and acknowledge their mental health care needs and the risks of and barriers to accessing care

- Develop strategies and priorities for improved care delivery
- Listen to and collaborate with Aboriginal and Torres Strait Islander peoples, and acknowledge concepts central to their mental, social and emotional wellbeing (for example, connection to culture)
- Routinely monitor, report on and evaluate processes, targets and measures of success to the governing body, workforce, community partners, and in the service provider's annual plan.

Implement, monitor, and report on strategies

The governing body is responsible for ensuring that the specific health needs of diverse population groups are identified and attuned to and for setting the priorities for the digital mental health services it will make available for these groups. Management is responsible for designing, implementing and monitoring the strategies to achieve these priorities, in collaboration with the communities they are serving.

Diverse population groups include:

- Culturally and linguistically diverse people
- Children and young people
- Older people
- Rural and remote populations
- LGBTIQ+ people
- People with disability.

Strategies for digital mental health services are most likely to be effective in best meeting individual needs when service users, consumers, carers, families, and support people from diverse population groups are actively engaged in their development, implementation, and evaluation.

Tasks for implementing the action:

- Review the membership of the governing body to ensure inclusion of representatives from diverse population groups
- Report on the safety and quality of digital mental health services delivered to diverse population groups to the governing body, workforce, the diverse population group communities, and in the service provider's annual plan
- Engage with consumers, carers, families, and communities of diverse population groups to identify relevant data for collection to inform planning and future decision-making relating to digital mental health services development and performance
- Routinely review data for safety and quality (including data relating to user experience, feedback, and complaints) and health outcomes for service users from diverse population groups
- Set goals or targets for utilisation by service users from diverse population groups, and routinely measure and report on specific performance indicators related to those goals and targets.

Review the scope and effectiveness of the digital mental health services in place to improve care for diverse population groups

The service provider should consider the role that digital mental health services can play in addressing the specific mental health needs of diverse population groups.

Tasks for implementing the action:

- Develop inclusive practice principles and inclusive language guidelines
- Provide digital mental health services that have the flexibility to meet diverse needs in areas including language, content, design and accessibility
- If possible, identify service users from diverse population groups who are receiving or may receive care via digital mental health services
- If applicable, identify service users for whom the digital mental health services would be contraindicated, and ensure that this information is included in the product information (see Action 3.03)
- In partnership with and informed by relevant cohorts, provide digital mental health services that are culturally sensitive and use images

and languages appropriate and relevant to the diverse population groups

- Evaluate the effectiveness of the digital mental health services in improving care for diverse population groups.

Examples of evidence

Examples of evidence may include:

Policy documents that incorporate the safety and quality needs and priorities for diverse population groups, including Aboriginal and Torres Strait Islander peoples

Documented goals and performance indicators for the targets and intended health outcomes for diverse population groups; these should be regularly monitored and reported to the governing body

Committee and meeting records that describe the safety and quality priorities and strategies for diverse population groups, including Aboriginal and Torres Strait Islander peoples

Evidence of previous or current engagement with Aboriginal communities about their mental health needs and priorities and their preferred strategies for digital mental health services

Examples of specific strategies that have been implemented to meet the needs of diverse population groups, including Aboriginal and Torres Strait Islander peoples

A current Reconciliation Action Plan, with reports of progress against actions in the plan

Role descriptions and recruitment processes for cultural consultants

Memorandum of understanding with partners from diverse population groups.

Related actions

This action relates to Action 1.15 (diversity) and Action 1.20 (cultural safety).

Useful resources

1. The National Safety and Quality Health Service Standards User Guide for Aboriginal and Torres Strait Islander Health. Available at: www.safetyandquality.gov.au/publications-and-resources/resource-library/nsqhs-standards-user-guide-aboriginal-and-torres-strait-islander-health[22]
2. Cultural Respect Framework 2016–2026 for Aboriginal and Torres Strait Islander Health: A national approach to building a culturally respectful health system. Available at: www.coaghealthcouncil.gov.au/Portals/0/National%20Cultural%20Respect%20Framework%20for%20Aboriginal%20and%20Torres%20Strait%20Islander%20Health%202016_2026_2.pdf[23]
3. The National Scheme's Aboriginal and Torres Strait Islander Health and Cultural Safety Strategy 2020–2025. Available at: https://nacchocommunique.files.wordpress.com/2020/02/aboriginal-and-torres-strait-islander-cultural-health-and-safety-strategy-2020-2025-1.pdf[18]
4. Framework for Mental Health in Multicultural Australia: Towards culturally inclusive service delivery. Available at: https://embracementalhealth.org.au/service-providers/framework-landing[24]
5. National Cultural Competency Tool for Mental Health Services[25]
6. Snapshot of mental health and suicide prevention statistics for LGBTI people, February 2020. Available at: www.lgbtiqhealth.org.au/statistics[26]
7. Equally Well Consensus Statement: Improving the physical health and wellbeing of people living with mental illness in Australia. Available at: www.equallywell.org.au/wp-content/uploads/2018/12/Equally-Well-National-Consensus-Booklet-47537.pdf[27]
8. Mental health of older Australians (in *Australia's welfare 2015*[28]). Available at: www.aihw.gov.au/getmedia/c2ff6c58-e05e-49ed-afd7-43bd21eef4e2/AW15-6-4-Mental-health-of-older-Australians.pdf.aspx
9. Mental health in rural and remote Australia. Available at: www.ruralhealth.org.au/sites/default/files/publications/nrha-mental-health-factsheet-dec-2017.pdf[29]
10. Health of people with disability (in *Australia's health 2020*[30]). Available at: www.aihw.gov.au/reports/australias-health/health-of-people-with-disability

Action 1.04

The service provider considers the safety and quality of health care for service users and their support people in its business decision-making.

Intent of the action

Business decisions put the safety and quality of care for service users and their support people first.

Reflective questions

- How are safety and quality issues considered when making business decisions?
- How are decisions about the safety and quality of care documented?

Meeting the action

Business decisions may centre on strategic and operational planning, service design, development and delivery of information security management systems, information and communication equipment, digital platforms, plant and buildings, staffing, and other resources.

Strategic and business planning

Review the service provider's strategic and business planning processes to ensure that they explicitly capture safety and quality improvement strategies and initiatives to be provided by digital mental health services.

Include safety and quality goals, objectives, and strategies for digital mental health services prominently in business and strategic plans.

Ensure that strategic and decision-making processes consider digital mental health services and consider the safety and quality of health care for service users and their support people when provided.

Business proposals

Review templates for submitting business proposals to the governing body and management and ensure that they provide for digital mental health services and take account of impacts on safety and quality.

If a proposal for development of a digital mental health service explicitly identifies implications for the safety and quality of health care for service users, adopt policies, procedures, or protocols to explain how clinical and technical risks will be managed.

Declare any affiliations, credentials, commercial interests (funders, investors and shareholders), conflicts of interest and disclaimers regarding the digital mental health services provided and record in minutes or a conflict-of-interest register.

Development and procurement specifications

Review the process for the development or procurement of digital mental health services, including any relevant contract templates, and ensure that requirements that support the clinical and technical safety and quality of digital mental health services are clearly defined and articulated.

Train the workforce to consider the safety and quality issues of digital mental health services when developing business cases or influencing business decisions.

Ensure the terms of reference for committees (for example, finance and audit committees, strategic planning committees) consider safety and quality implications of digital mental health services when making business decisions.

Ensure that decisions about the information security management systems, information and communication equipment, digital platforms, plant and buildings are informed. Also ensure that products and services are fit for purpose, comply with relevant standards, and take into consideration safety and quality issues such as privacy, data security and data usage.

Examples of evidence

Examples of evidence may include:

Committee and meeting records – such as those from finance, audit and strategic planning committees – that show that the safety and quality of digital mental health care is considered in business decision-making

Strategic plans, operational plans or business plans that outline the potential impact of decisions on the safety and quality of care on service users

Business proposal templates that include consideration of safety and quality risks

A register of safety and quality risks that includes actions to manage the identified risks

A conflict-of-interest register.

Related actions

This action relates to Action 1.25 (terms and conditions).

Useful resources

1. Cybersecurity resources. Available at: www.digitalhealth.gov.au/healthcare-providers/cybersecurity[31]

Action 1.05

The service provider applies ethical principles to its business decision-making about the design, development, and delivery of services.

Intent of the action

The design, development, and delivery of digital mental health services are in line with the service provider's endorsed ethical principles.

Reflective questions

- How are ethical principles applied when making business decisions?

Meeting the action

Endorse ethical principles for digital mental health services

Ethics look at what actions are right or wrong in particular circumstances. The principles of ethical behaviour include non-maleficence (not causing harm), beneficence (doing good), autonomy (making one's own decisions), and justice (fairness and equity). Ethical codes developed by professional organisations are typically built on ethical principles and values such as fairness, accountability, responsibility, reliability, integrity, and honesty.[32]

The service provider should demonstrate ethical behaviour, practices, and policies in professional contexts[33], taking account of cultural factors for the communities in scope. Information ethics addresses the uses and abuses of information, information technology, information systems and the use of information in decision-making, and creates ethical standards and rules for processing, storing, and sharing information. For information systems, ethical questions include whether an information system is fair and compatible with stakeholders' ethical values.[34]

Having an ethical frame of reference therefore allows a service provider to make decisions about the proper use of technology, and whether it is appropriate and is used for public good.

Issues such as privacy, security, equality, accessibility, and data protection are some ethical concerns posed by digital mental health technologies. Those involved in the design, development and delivery of digital mental health technologies and applications should use an ethical frame of reference to guide their decisions as to what makes for ethical practice and what code of ethics they will adhere to. For example, applying ethical principles can help ensure that digital mental health services are safely made available to service users and can prevent data derived from those services from being misused.

Published case studies can assist in explaining the ethical issues that arise in digital mental health services and how the application of ethical principles can inform business decisions about the design, development, and delivery of digital mental health services.

Tasks for implementing the action:

- Endorse ethical principles and values to guide the service provider's business decision-making about digital mental health services
- Engage service users, consumers, carers, families, and their support people in the development and implementation of the ethical framework
- Periodically review ethical principles and values in collaboration with service users, consumers, carers, families, and support people, to ensure that they continue to guide consideration of the latest issues relevant to achieving safety and quality in digital mental health service delivery

- Reference the ethical principles and values in business and strategic plans and periodically review strategic planning and business planning processes to ensure that they are consistent with the ethical framework and prompt consideration of ethical issues
- Train the workforce to recognise and consider the ethical issues that might arise when developing business cases for digital mental health services.

Design, develop and deliver ethical services

Review templates for submitting business proposals to the governing body and management, and ensure that they provide for ethical matters in the design, development, and delivery of digital mental health services.

Determine clear specifications to ensure that any digital mental health service provided meets the ethical principles and values endorsed by the service provider.

Report on any ethical issues in the design, development, and delivery of digital mental health services provided.

Examples of evidence

Examples of evidence may include:

Committee and meeting records – such as those from finance, and strategic planning committees – that show that ethics is considered in business decision-making

Strategic plans, operational plans or business plans that outline ethical issues and their potential effect on service users

Business proposal templates that include consideration of ethical matters

Policy documents that include the organisation's ethical framework and principles, possibly including whistle blower provisions

A code of conduct that outlines ethical principles and the standard of behaviours and actions expected.

Useful resources

1. IEEE 7000-2021 – IEEE Standard Model Process for Addressing Ethical Concerns During System Design. Available at: https://engagestandards.ieee.org/ieee-7000-2021-for-systems-design-ethical-concerns.html?utm_source=ieeesa&utm_medium=aem&utm_campaign=ais-2021[35]
2. Responsible Innovation in Online Therapy. Available at: https://doi.org/10.17863/CAM.4584136[36]
3. Ethics and law for the health professions (4th ed.)[37]

Clinical and technical leadership

Action 1.06

The service provider:

a. Ensures clinical, peer worker and technical leaders understand and perform their delegated safety and quality roles and responsibilities
b. Ensures clinical, peer worker and technical leaders operate within the clinical and technical governance frameworks to improve the safety and quality of health care for service users and their support people
c. Engages clinical and peer worker expertise in the clinical governance of the service
d. Engages technical expertise in the technical governance of the service.

Intent of the action

Service providers work with clinical, peer worker and technical leaders to optimise the safety and quality of care delivered by digital mental health services.

Reflective questions

- How do clinical leaders contribute to the clinical governance of the service?
- How do peer workers contribute to clinical and technical governance of the service?
- How do technical leaders contribute to the technical governance of the service?
- How does the service provider ensure that the workforce operates within the clinical and technical governance frameworks?

Meeting the action

Strong leadership can drive safety and quality improvements and make them a priority. Commitment from leaders is important, because their actions and attitudes influence the decisions of the organisation and the perceptions, attitudes, and behaviours of the workforce.

Define safety and quality roles and responsibilities

Consult with the clinical, peer worker and technical workforce to define and allocate their delegated safety and quality roles and responsibilities, including:

- Implementing strategic directions about digital mental health services
- Managing the operation of the clinical and technical governance systems
- Reporting on safety and quality
- Supporting the organisation's safety culture.

Reporting lines and relationships for safety and quality performance should be clearly documented.

Train the workforce

Provide safety and quality training for clinical, peer worker and technical leaders.

Ensure that the broader workforce has access to information about their expected roles and responsibilities for safety and quality of digital mental health services, and for the operation of the clinical and technical governance framework.

Provide leadership

Clinical, peer worker and technical leaders may support the delivery of the digital mental health services by:

- Supervising relevant members of the workforce
- Conducting performance appraisals or peer reviews
- Reviewing safety and quality performance data of digital mental health services and benchmarking these data
- Ensuring that the workforce supporting the provision of the digital mental health services understands the clinical and technical governance system
- Working with business management leaders to optimise the clinical and technical outcomes within the working environment.

Review results

Review clinical and technical audit results and deal with any issues identified.

Ensure that mechanisms are in place to receive reports on performance and clinical and technical incidents. Make sure clinical, peer worker and technical leaders are engaged in the review of performance, incidents, and adverse events.

Examples of evidence

Examples of evidence may include:

Policy documents that outline the delegated safety and quality roles and responsibilities of clinical and technical leaders

Documents that outline the leadership capability framework

Employment or contract documents that describe the safety and quality roles and responsibilities of clinical and technical leaders

Documented workforce performance appraisals or contract reviews that include feedback to clinical and technical leaders on the performance of safety and quality roles and responsibilities

A code of conduct that outlines the standard of expected behaviours and actions

Training documents relating to workforce safety and quality roles and responsibilities

Results of clinical and technical audits of the performance of the workforce under the clinical and technical governance frameworks

Documented results of clinical and technical audits, and actions taken to deal with any identified issues

Policy documents that outline performance review and performance management processes.

Useful resources

1. National practice standards for the mental health workforce 2013. Available at: www.health.gov.au/resources/publications/national-practice-standards-for-the-mental-health-workforce-2013[38]

Criterion: Safety and quality systems

Safety and quality systems are integrated with governance processes to enable the service provider to actively manage and improve the safety and quality of care.

Effective clinical and technical governance creates a learning environment and a comprehensive program of continuous quality improvement. The service provider's safety and quality systems should ensure that safety and quality incidents associated with digital mental health services are recognised, reported, and analysed, and used to improve the digital mental health services and care provided. Incidents may be clinical (for example, an episode of self-harm during care) or technical (for example, a data breach or an unplanned interruption of the service). It is important that these systems are integrated with governance processes. This enables service providers to actively manage risk, and to improve the safety and quality of digital mental health services.

The service provider's approach to delivering and supporting information and care provided by digital mental health services should be described in policies, procedures and protocols, which may need to be endorsed by the governing body. These documents should include the following topics:

- Developing policies, procedures and protocols
- Monitoring and reporting clinical and technical performance
- Managing clinical and technical risk
- Managing complaints and compliments
- Managing open disclosure
- Engaging clinicians, peer workers, and technicians in planned, systematic audits of digital mental health services following agreed protocols and schedules.

Legislation, regulations, policies and procedures

Action 1.07

The service provider uses a risk management approach to:

a. Set out, review, and maintain the currency and effectiveness of policies, procedures and protocols
b. Monitor and take action to improve adherence to policies, procedures and protocols
c. Review compliance with legislation, regulations, and jurisdictional requirements.

Intent of the action

The service provider has current, comprehensive and effective policies, procedures and protocols that cover safety and quality risks and compliance with legislation and regulations.

Reflective questions

- How does the service provider ensure that its policy documents are current, comprehensive, and effective?
- How does the service provider ensure that its policy documents comply with legislation, regulations, and national, state or territory requirements?

Meeting the action

Develop policies, procedures and protocols

The governing body must clearly delegate responsibility for developing and maintaining policies, procedures and protocols about digital mental health services. The content and scope of this suite of documents will vary depending on the size of the service provider and the type, context, complexity and risk of the digital mental health services it offers.

Tasks for implementing the action:

- Set up a comprehensive suite of policies, procedures and protocols that emphasises the safety and quality of digital mental health services; the suite should cover clinical and technical safety and quality risks and be consistent with the service provider's regulatory obligations
- Incorporate all policy, procedure and protocol documents relating to digital mental health services into a single coherent suite to maximise the effectiveness of the policy development process
- Identify a custodian to ensure that the processes for developing, reviewing, and monitoring compliance with policies, procedures and protocols are documented, along with the roles and responsibilities of individuals and committees with the authority to amend or endorse each policy, procedure, or protocol
- Set up mechanisms to maintain currency of policies, procedures and protocols, and to communicate changes in them to the workforce
- Ensure that the workforce has ready access to relevant policies, procedures and protocols
- Develop position descriptions, contracts, bylaws, or other mechanisms that require the workforce to comply with their roles, responsibilities, and accountabilities,

and with organisational policies, procedures and protocols.

Monitor compliance with legislation, regulation, and national, state or territory requirements

Periodically review the use and effectiveness of organisational policies, procedures and protocols through audits or performance reviews. Ensure that they reflect best practice and current evidence and align them to national and state or territory legal and policy requirements.

Develop or adapt a legislative compliance system that incorporates a compliance register to ensure that policies, procedures and protocols are regularly and reliably updated, and that they respond to relevant regulatory changes, compliance issues, and case law.

Record instances of noncompliance with relevant legislation or regulations, or the organisation's policies, procedures and protocols relating to digital mental health services. Where appropriate, incorporate this information into the organisation's risk register and quality improvement planning processes.

Identify relevant industry standards, and develop processes to implement and monitor compliance with relevant standards, legislation and guidelines. Such industry standards may include:

- Relevant service-specific standards such as those dealing with mental health, suicide prevention and abuse of alcohol and other drugs
- Standards Australia standards
- International Organization for Standardization (ISO) standards
- Guidance developed by peak bodies, such as the Royal Australian and New Zealand College of Psychiatrists and the Australian Psychological Society
- Therapeutic Goods Administration (TGA) regulation of software as a medical device
- Commonwealth, state and territory privacy and health records legislation
- Australian consumer law.

Meet Australian consumer law

Australian consumer law requires all products supplied to consumers to be safe, fit for purpose, and to meet consumer guarantees. If the product is unsafe or does not do what is promised, the consumer is entitled to a refund and may also seek compensation for damages and loss caused by a safety defect.

There are also two mandatory notification requirements:

- If there is a risk that a product will or may cause injury, it must be recalled
- If there is awareness of a death, serious injury or illness associated with a supplied product, the supplier must report it within two days. All participants in the supply chain of a consumer good are required to comply with the reporting requirement.[39]

The service provider should implement processes to comply with mandatory notification requirements and report on this to the governing body.

Examples of evidence

Examples of evidence may include:

Documented processes for developing, authorising, and monitoring the implementation of the service provider's policy documents

A register of policy document reviews, including the date of effect, dates that policy documents were amended, and a prioritised schedule for review

Examples of policy documents that have been reviewed in response to identified risks, or changes in legislation, regulation, or best practice

Committee and meeting records that describe the governance structure, delegations, roles, and responsibilities for overseeing the development of policy documents

Results of audits of healthcare records and clinical practice for compliance with policy documents

Results from workforce surveys and feedback on policy documents

Data and feedback from risk management, incident management and complaints management systems, and evidence that these data are used to update policy documents

Communication with the workforce on new or updated policy documents

Training documents on new or amended policy documents or use of policy documents

Schedules and timelines for statutory reporting.

Useful resources

1. A Health App Developer's Guide to Law and Policy (Appendix 1 of Finding peace of mind: Navigating the marketplace of mental health apps[40]. Available at: https://accan.org.au/grants/completed-grants/1256-mental-health-apps
2. National practice standards for the mental health workforce 2013. Available at: www.health.gov.au/resources/publications/national-practice-standards-for-the-mental-health-workforce-2013[38]
3. Mental health legislation and psychiatrists: putting the principles into practice. Available at: www.ranzcp.org/news-policy/policy-and-advocacy/position-statements/mental-health-legislation-and-psychiatrists[41]

Measurement and quality improvement

Action 1.08

The service provider uses quality improvement systems that:

a. Identify safety, outcome, and quality measures, and monitor and report performance and outcomes
b. Identify areas for improvement in safety and quality
c. Maintain a quality improvement register to log initiatives to improve safety and quality
d. Assign to members of the workforce clear responsibility for safety and quality
e. Implement and monitor safety and quality improvement initiatives.

Intent of the action

An effective quality improvement system is operating for digital mental health services, and includes improvement of service user experience and outcomes.

Reflective questions

- How does the quality improvement system reflect the service provider's safety and quality priorities and strategic direction?
- How does the service provider identify and document safety and quality risks and opportunities for improvement?
- What processes are used to ensure that the actions taken to manage identified risks and improvements are effective?

Meeting the action

Develop a quality improvement system

Tasks for implementing the action:

- Clearly describe the clinical and technical quality objectives and how they align with the organisation's objectives
- Clearly define the processes and responsibilities that are required to meet the quality objectives
- Involve service users, consumers, carers, families and support people, along with clinical, peer worker and technical experts in the quality improvement systems
- Maintain a quality improvement register for digital mental health services; ensure it is informed by outcomes and performance, incidents, feedback, complaints, audits, and reviews
- Establish mechanisms for monitoring service user satisfaction and outcomes and using that information to inform improvements
- Train the workforce in clinical and technical safety and quality

- Periodically review the quality improvement system to:
  - verify that it is operating effectively for both clinical and technical aspects of digital mental health services
  - ensure that it reflects the service provider's current clinical and technical safety and quality priorities, and its strategic direction for digital mental health services.

Define clinical and technical safety and quality

Involve service users, consumers, carers, families and support people, and also clinical, peer worker and technical experts in defining clinical and technical safety and quality.

Reflect this definition throughout the organisation's vision, mission and values, and share this information with the workforce.

Define indicators and outcome measures

Define the outcome measures and safety and quality indicators for digital mental health services that will be routinely collected and reported. These may include measures and indicators relating to:

- Access
- Clinical effectiveness
- Safety
- Data security
- Service user outcomes and their experiences of care
- Clinical incidents and near misses
- Technical incidents and near misses
- Complaints management
- Compliance with best-practice pathways
- Compliance with relevant regulatory requirements.

Provide training and education to the workforce on these indicators and measures.

Decide how feedback about clinical and technical aspects will be collected from the workforce, service users and their support people, and external peer workers or clinicians who refer to or use the service provider's digital mental health services.

Conduct regular reviews and audits

Audits are effective if their outcomes are used for improvement and assurance purposes. Independent auditors or reviewers can help ensure a high level of assurance of objective reporting for the governing body.

Tasks for implementing the action:

- Develop a schedule of reviews and audits that covers the clinical and technical aspects of the delivery of care and provides systematic oversight of safety and quality systems
- Conduct clinical and technical audits that test the design and performance of the clinical and technical governance system
- Actively engage with the clinical, peer worker, and technical workforce, and service users and their support people in the audit processes and analysis of results
- Record the outcomes of clinical and technical system audits on a register, together with proposed actions and responsibilities, and evidence of implementation and follow-up; these records can be used to show how risks and opportunities identified through the quality improvement system are addressed to continuously improve safety and performance.

Examples of evidence

Examples of evidence may include:

Policy documents that describe the processes and accountability for monitoring the safety and quality of services

Documented safety and quality performance measures

A schedule for internal or external audits

Audit reports, and presentations of analysis of safety and quality performance data

Feedback from the workforce about the use of safety and quality systems

Feedback from service users about their involvement in the review of safety and quality performance data

A quality improvement register and a plan that includes actions to deal with issues identified

Examples of specific quality improvement activities that have been implemented and evaluated

Committee and meeting records in which reports, presentations, and safety and quality performance data are regularly reviewed and reported to the governing body or relevant committees

Training documents about the service provider's quality improvement system

Communication with the workforce and service users that provides feedback about safety and quality of services

Published research on digital mental health service safety, outcomes and quality.

Action 1.09

The service provider ensures timely reports on safety and quality systems and performance are provided to:

a. The governing body
b. The workforce
c. Service users and their support people.

Intent of the action

Accurate and timely information on clinical and technical safety and quality performance of digital mental health services is provided to key stakeholders.

Reflective questions

- What processes are used to ensure stakeholders are provided with accurate and timely information about safety and quality performance?

Meeting the action

Routinely collecting process and outcome data, monitoring trends and performance, and reporting regularly enables service providers to understand outcomes from digital mental health service delivery, identify areas that require attention (such as deviations from the expected outcomes), and respond promptly. The monitoring of safety and quality performance data should include relevant clinical and technical areas to ensure a comprehensive picture of performance.

Document processes for monitoring and reporting

Collaborate with the workforce, service users and their support people, referrers, and other relevant stakeholders to define the topic areas, format, and frequency of reporting.

Clearly document processes to ensure the accuracy, validity, and comprehensiveness of information and increase confidence in data quality.

Report regularly

Reports should be tailored to the intended audience and take account of health and digital literacy levels. Reports for service users may take a different form and use simpler language than those prepared for the governing body or management. The frequency of reporting should be determined by the service provider and take account of the nature of the digital mental health service, its volume of use, and the metrics available for reporting.

Tasks for implementing the action:

- Develop a schedule for reporting and managing the design and performance of key clinical and technical systems
- Report regularly to the governing body, the workforce, and service users and their support people
- Monitor and review progress on actions taken to improve clinical and technical safety and quality, and provide feedback to service users and the workforce
- Provide information and training to the workforce and users of digital mental health services to encourage their involvement in the analysis of performance data.

Examples of evidence

Examples of evidence may include:

Reports on safety and quality performance data that are provided to the governing body, the workforce or service users

Committee and meeting records in which safety and quality indicators, data or recommendations by the governing body are discussed

Committee and meeting records in which the appropriateness and accessibility of the service provider's safety and quality performance information are discussed

A communication strategy that describes processes for disseminating information about safety and quality performance

Communication with the workforce and service users and their support people about the service provider's safety and quality performance

Records of safety and quality performance information published in annual reports, newsletters or other media

Reporting templates and calendars.

Risk management

Action 1.10

The service provider:

a. Identifies and documents service risks
b. Uses clinical, technical, and other data collections to support risk assessments
c. Acts to reduce risks
d. Regularly reviews and acts to improve the effectiveness of the risk management system
e. Reports on risks to the workforce, and service users and their support people
f. Plans for and manages internal and external emergencies and disasters, including cybersecurity risks and threats.

Intent of the action

The service provider identifies and manages risk effectively.

Reflective questions

- How does the service provider identify and document risk?
- What processes does the service provider use to set priorities for, and manage, risks?
- How does the service provider use the risk management system to improve safety and quality?

Meeting the action

Define the governing body's responsibility

The governing body is responsible for ensuring the integrity of the risk management system for digital mental health services. The governing body should:

- Determine the service provider's risk appetite and tolerance – that is, the amount and type of risk that the organisation is willing to take to meet its strategic objectives in relation to digital mental health services
- Document the risk management system in policies, procedures and protocols that define a vision, principles, objectives, practices, responsibilities, resources, and how outcomes will be measured
- Allocate resources to support the risk management system
- Foster an organisational culture that focuses on clinical and technical safety and continuous improvement in identifying and managing risk
- Ensure appropriate integration of the management of clinical and technical risks.

Embed a systems approach to risk management

Key tasks for implementing the action:

- Maintain risk management policies, procedures and protocols that identify the sources of information required to reliably assess risk and clearly allocate roles, responsibilities, and accountabilities
- Establish a reliable and systematic process of hazard identification across all areas related to digital mental health services
- Actively encourage and support the workforce, service users and their support people, and other stakeholders to report potential and actual risks
- Maintain a comprehensive, accurate and current risk register, which can be used as a practical tool for risk management
- Assign all risks to a risk owner, who is responsible for managing and monitoring risks, and ensuring that appropriate accountability arrangements are in place
- Regularly review risks and report on risk to the governing body, the workforce, and service users and their support people
- Establish a reliable system to scan for, identify and respond to hazards and risks reported by other organisations, government agencies, insurers, coroners, or in the scientific literature
- Conduct a planned, systematic program of in-house and external audits or reviews on the design and performance of safety and quality systems, in collaboration with clinicians, technicians, and service users and their support people, and incorporate this risk audit program into the formal audit program
- Ensure that the risk management system includes strategies, resources, and clear accountability for remedying risks
- Periodically review the effectiveness of the risk management system and monitor and assess performance regarding risk, within a defined performance monitoring framework, at all levels of the organisation, including the governing body and management.

Engage the workforce

Fostering the engagement and participation of the workforce will help to identify clinical and technical risks associated with digital mental health services.

Tasks for implementing the action:

- Systematically provide appropriate information, orientation, education and training to the workforce using the risk management system
- Reinforce information about roles, responsibilities and accountabilities for reporting and managing risk to managers, clinicians, peer workers, technical experts, and other members of the workforce
- Establish within the committee structure responsibility for systematic risk identification, assessment, review, and management of digital mental health service–related risks
- Use routine meetings as an opportunity to identify and discuss clinical and technical safety concerns
- Include digital mental health services' safety as a standing item on meeting agendas of the governing body and management.

Plan for and manage emergencies and disasters

Use a risk management approach to plan for emergencies and disasters that may affect the service provider's operation of digital mental health services or the safety of service users and their support people. This includes cybersecurity risks and threats, and data breaches.

Perform audits to identify potential risks and management opportunities to enable the organisation to respond efficiently and effectively in an emergency. This may involve:

- Installing appropriate infrastructure, such as backup servers to enable digital systems to continue working
- Training the workforce in emergency drills
- Planning for the coordination of workforce rosters and reporting lines during an emergency

- Business continuity planning for recovery and returning services to normal following an emergency.

Examples of evidence

Examples of evidence may include:

Policy documents that describe the processes for implementing and monitoring the risk management system

Policy documents that describe the reporting lines, and roles and responsibilities of the workforce when dealing with emergencies and disasters

A risk register that includes actions to manage identified risks

Reports on safety and quality data that are analysed to identify and monitor safety and quality risks

Data analysis and reports on safety and quality performance trends

Feedback from the workforce on safety and quality risks, and the effectiveness of the risk management system

Committee and meeting records about oversight of the risk management system, or the review of clinical, technical, and other data collections

Committee and meeting records in which risk, and the appropriateness and accessibility of safety and quality performance information are discussed

Audit schedule and reports on compliance with the policies, procedures and protocols of the service provider's risk management system

Communication with the workforce and service users and their support people on risks and risk management

Published records of safety and quality performance information – for example, annual reports, newsletters, newspaper articles, radio items, and websites

A business continuity plan, or emergency and disaster management plan

Training documents about risk management, and the management of emergencies and disasters, including cybersecurity risks and threats.

Useful resources

1. ISO 31000, Risk management. Available at: www.iso.org/iso-31000-risk-management.html[42]
2. Data Backup and Restoration (in Guidelines for System Management[43]). Available at: www.cyber.gov.au/acsc/view-all-content/advice/guidelines-system-management
3. Information Security Guide for small healthcare businesses. Available at: www.digitalhealth.gov.au/sites/default/files/2020-11/Information_security_guide_for_small_healthcare_businesses.pdf[44]

Incident management systems and open disclosure

Action 1.11

The service provider has incident management and investigation systems and:

a. Assists the workforce to recognise and report incidents
b. Assists service users and their support people to communicate concerns or incidents
c. Involves the workforce, consumers, carers, and families in the review of incidents
d. Provides timely feedback on the analysis of incidents to the governing body, the workforce, and service users and their support people
e. Uses the information from the analysis of incidents to improve safety and quality
f. Incorporates risks identified in the analysis of incidents into the risk management system
g. Regularly reviews and acts to improve the effectiveness of the incident management and investigation systems.

Intent of the action

Clinical and technical incidents are identified and managed appropriately, and action is taken to improve safety and quality.

Reflective questions

- How does the service provider identify and manage incidents?
- How are the workforce and service users involved in reviewing incidents?
- How is the incident management and investigation system used to improve safety and quality?

Meeting the action

Incident reporting can improve safety and care processes, change the way the workforce thinks about risk, and raise awareness of good practices. The nature of the risks faced will vary according to the service provider and the context of their digital mental health service delivery.

Implement a comprehensive incident management and investigation system

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 appropriately designed, resourced, maintained, and monitored.

Tasks for implementing the action:

- Define what constitutes a clinical incident, a technical incident, and a near miss
- Develop a clear policy framework that defines the key elements of the incident management and investigation system, including the:
  - roles and responsibilities of individuals and committees
  - types of events to be reported
  - processes for reporting, responding to, investigating, analysing and monitoring clinical and technical incidents and near misses

  - responsibilities of clinicians, peer workers, and technicians to report incidents and near misses they observe or that arise from the use of digital mental health services
- Ensure that the policies, procedures and protocols protect the confidentiality of information and allow incidents to be reported anonymously
- Set up classification and escalation processes to ensure that serious incidents, and incidents associated with major risk are managed appropriately, including external reviews, if required
- If applicable, link the incident management system to the:
  - service provider's open disclosure, risk management, credentialing and scope of practice processes
  - state or territory incident management and investigation system
- Develop a procedure for communicating incidents to the service provider's professional indemnity insurers
- Designate an individual with responsibility for maintaining the integrity of the incident management system and for coordinating incident management and investigations
- Manage each incident appropriately from a clinical and technical perspective and ensure the provision of safe, high-quality care to the service user and, if relevant, their support people following the incident, including open disclosure if appropriate
- Periodically review the design and performance of the incident management and investigation systems to ensure that they are effective in improving safety, comply with best-practice design principles, and that the resources allocated support effective clinical and technical governance and risk management.

Support the workforce

Leaders, including clinical, peer worker, and technical leaders, should encourage the workforce to use the incident management system to report clinical and technical incidents and near misses.

Tasks for implementing the action:

- Provide information about the intent and use of the incident management and investigation systems to the workforce at orientation and routinely throughout their employment
- Engage the workforce to find solutions to issues.

Support service users and their support people

Inform service users and their support people about how they can report incidents or concerns.

Tasks for implementing the action:

- Distribute information to service users and their support people about the types of incidents and concerns and how to report them
- Train the workforce on how to respond to service users and their support people who raise concerns or report incidents
- Provide appropriately skilled members of the workforce to liaise with service users and their support people who report concerns or incidents
- Seek feedback on safety incidents from service users and their support people; for example, through surveys
- Provide information about improvement activities that have been implemented based on service user feedback.

Review incidents

Appropriate review of incidents enables lessons to be learned and improvements to be implemented.

Tasks for implementing the action:

- Engage the clinicians, peer workers, and technicians involved in an incident, and the manager responsible for the digital mental health service, to review each incident
- Establish a system to verify that managers follow up incidents appropriately to ensure integrity of the risk management system.

Report on incidents

Tasks for implementing the action:

- Analyse clinical and technical incident and near-miss data to identify trends and find opportunities for improvement
- Define a reporting framework that clearly identifies the data that will be available and reported by the service provider, and where it will be reported
- Ensure that the reporting of information about clinical and technical incidents and near misses is prompt and effective
- Provide comprehensive information to the governing body and management on all serious incidents, and summary information about all other incidents; include information such as the actions taken because of a specific incident or category of incidents, and indicators such as time to complete actions stemming from incident reports
- Provide reports to the workforce and service users, consumers, carers, families, and support people on clinical and technical incidents and near misses
- Report incidents to other parties as required under legislation, including notifiable data breaches under the Privacy Act, and other obligations – for example, to funders.

Examples of evidence

Examples of evidence may include:

An incident management and investigation system in which clinical and technical incidents are documented, analysed, and reviewed

Policy documents about reporting, investigating and managing clinical and technical incidents

Information on clinical and technical incidents and the actions taken to manage identified risks, and how these actions are incorporated into the service provider's risk management system or quality improvement plan

Training documents about recognising, reporting, investigating and analysing incidents, adverse events and near misses

Committee and meeting records that describe the incident management and investigation system, and the strategies and actions to reduce risk

Committee and meeting records that show workforce and service user involvement in the analysis of organisational safety and quality performance data

Clinical and technical incident reporting forms and tools that are accessible to the workforce and service users

Information and resources that support the workforce and service users to report clinical and technical incidents

Feedback from the workforce and service users about their involvement in the review and analysis of organisational safety and quality performance data

Examples of specific improvement activities that have been implemented and evaluated to reduce the risk of incidents identified through the incident management and investigation system
Results of completed clinical or technical incident investigations
Audit results showing compliance with the incident management and investigation system.

Useful resources

1. Data breach action plan for health service providers. Available at: www.oaic.gov.au/privacy/guidance-and-advice/data-breach-action-plan-for-health-service-providers[45]
2. Best practice guide to clinical incident management. Available at: https://clinicalexcellence.qld.gov.au/sites/default/files/2018-01/clinicalincidentguide.pdf[46]
3. Incident management policy resources. Available at: www.cec.health.nsw.gov.au/Review-incidents/incident-management-policy-resources[47]

Action 1.12

The service provider:

a. Uses an open disclosure program that is consistent with the Australian Open Disclosure Framework

b. Monitors and acts to improve the effectiveness of open disclosure processes.

Intent of the action

An open disclosure process is used to enable the service provider, clinicians and its peer workers and technicians to communicate openly with service users and, if relevant, their support people, about unexpected healthcare outcomes or harm from using its services.

Reflective questions

- How is the workforce trained and supported to discuss incidents that have caused harm to service users?
- How is information from the open disclosure program used to improve safety and quality?

Meeting the action

Open disclosure is a discussion with a 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:

- An obligation of the service provider
- A normal part of care, should the unexpected occur
- A reasonable expectation of service users
- An attribute of a high-quality service provider and an important part of healthcare quality improvement.

An open disclosure discussion should include:

- The elements of an apology or expression of regret (including the word 'sorry')
- A factual explanation of what happened
- An opportunity for the service user to relate their experience
- An explanation of the steps being taken to manage the event and prevent a recurrence.

Endorse and implement open disclosure framework

Tasks for implementing the action:

- Develop or adapt policies, procedures and protocols that are consistent with the Australian Open Disclosure Framework[48] in a way that reflects the context of the digital mental health service provision
- Allocate resources to support implementation of the open disclosure framework
- Lead a 'just culture' marked by openness and constructive learning from mistakes
- Assign responsibility for implementing the framework to an individual or committee
- Train members of the workforce who will be involved in open disclosure
- Provide access to support for relevant members of the workforce who have responsibility for managing issues involving open disclosure within the organisation
- Monitor open disclosure events to ensure they are followed up and remediations and improvements are actioned

- Regularly report on open disclosure to the governing body, including on the learnings from system errors that caused poor outcomes for service users or their support people
- Audit compliance against the open disclosure framework to ensure that the principles and processes of the framework are met, and investigate and deal with all variations from the framework
- Review open disclosure events to find out how the open disclosure program could be improved.

Examples of evidence

Examples of evidence may include:

Policy documents that are consistent with the principles and processes outlined in the Australian Open Disclosure Framework

Reports by the service provider about open disclosure events

Information and data on open disclosure presented to the governing body and relevant committees

Committee and meeting records about issues and outcomes related to open disclosure.

Useful resources

1. Australian Open Disclosure Framework. Available at: www.safetyandquality.gov.au/our-work/open-disclosure/the-open-disclosure-framework[48]

Feedback and complaints management

Action 1.13

The service provider:

a. Has processes to seek regular feedback from service users and their support people about their experiences of the service and outcomes of care

b. Uses this information to improve safety, quality, performance, and effectiveness.

Intent of the action

Feedback from the workforce, service users and their support people is used to improve the safety and quality of digital mental health services.

Reflective questions

- How does the service provider collect service user experience feedback?
- How does the service provider collect feedback from the workforce?
- How are service user experience data and workforce feedback used to improve safety and quality?

Meeting the action

Reports by service users and their support people of their experiences of care are important for determining the quality of care provided. Feedback should be gathered systematically, using well-designed data collection tools and the data used to improve the quality of care. Feedback should be collected in a culturally appropriate way.

Decide on the feedback method

Adopt a validated and reliable method to regularly and systematically seek feedback from service users and their support people; for example:

- A validated survey instrument
- Focus groups of service users that can consider specific issues, or issues relating to a specific digital mental health service.

Implement a comprehensive feedback system

Tasks for implementing the action:

- Allocate resources to support the feedback system
- Designate an individual to be responsible for maintaining the integrity of feedback systems
- Provide cultural safety training for relevant staff to ensure that feedback is collected in a culturally safe way
- Regularly seek service user feedback
- Analyse the information gained from the feedback system for safety and quality risks and improvement opportunities, and ensure the service provider's quality improvement system responds to the issues identified
- Regularly report to the governing body on the analysis of service user experience data and the actions taken to deal with the concerns identified
- Provide the workforce, service users and their support people with information about what has been learned from the feedback system, and how it has led to improvements
- Compare performance with similar services and any nationally available benchmarks
- Periodically review the performance and effectiveness of the service user's feedback system.

Examples of evidence

Examples of evidence may include:

Tools used for collecting service user feedback

Committee or meeting records about the selection of service user experience questions, and review of service user feedback

Data analysis and reports of service user feedback or surveys used to evaluate the service provider's performance

Strategic, business and quality improvement plans that incorporate service user feedback.

Action 1.14

The service provider has a complaints management system, and:

a. Encourages and assists service users and their support people to report complaints
b. Involves service users and their support people in the review of complaints
c. Resolves complaints in a timely way
d. Provides timely feedback to the governing body, the workforce, and service users and their support people on the analysis of complaints and actions taken
e. Uses information from the analysis of complaints to inform improvements in safety and quality
f. Records the risks identified from the analysis of complaints in the risk management system
g. Regularly reviews and acts to improve the effectiveness of the complaints management system.

Intent of the action

An effective complaints management system is in place and used to improve safety and quality of digital mental health services.

Reflective questions

- What processes are used to ensure that complaints are received, reviewed, and resolved in a prompt and compassionate manner?
- How are complaints data used to improve safety and quality?
- What processes are used to review the effectiveness of the complaints management system?

Meeting the action

Implement a complaints management system

A comprehensive complaints management and investigation system should be designed and implemented to take advantage of the opportunities for improvement that complaints provide.

Tasks for implementing the action:

- Develop a clear policy framework that defines the key elements of the complaints management and investigation system, including the:
  - roles and responsibilities of individuals and committees
  - processes for receiving, investigating, and managing complaints, and taking immediate action if required
  - process for feeding back to the complainant to close the loop following investigation and management of a complaint
  - process for confidential and anonymous reporting of complaints

- Link the complaint management system to the service provider's policies on open disclosure, risk management, credentialing and scope of practice (if applicable), and quality improvement systems
- Develop a procedure for communicating complaints to the service provider's professional indemnity insurer
- Designate an individual or committee with responsibility for maintaining the integrity of the complaints management system and for coordinating complaint management
- Develop risk-based classification and escalation processes to ensure that complaints are managed appropriately
- Maintain a complaint register to ensure that complaints are managed efficiently and effectively, and that each complaint process is completed
- Communicate effectively with complainants about the management of their complaint (if possible)
- Periodically review the design and performance of the complaints management system to ensure it is effective in improving safety and complies with best-practice design principles.

Support service users, their support people, and the workforce

Encourage the workforce, service users and their support people to report complaints.

Tasks for implementing the action:

- Develop a statement about the service provider's approach to complaints management, including:
  - how complaints are managed
  - expected time frames for investigation
  - how the complainant will be notified of the outcome of the investigation, if possible
  - how a service user can make a complaint to an appropriate independent complaints body
- Provide information to the workforce, service users and their support people about how to make a complaint along with the statement about the service provider's approach to complaints management
- Provide training for service users and the workforce on complaints handling (including cultural safety in handling complaints) and the data and measurements used by the service provider.

Review complaints

Appropriate review of complaints enables lessons to be learned and improvements to be implemented.

Tasks for implementing the action:

- Ensure prompt and effective review of complaints, in line with the service provider's policies, procedures or protocols
- Engage the member(s) of the workforce involved and the manager responsible for the digital mental health service about which the complaint was generated in the review of the complaint
- Invite members of the workforce, service users, consumers, carers, families and support people to join groups or committees responsible for reviewing complaints or safety and quality performance data
- Implement a system to verify that managers follow up complaints appropriately to ensure the integrity of the complaints management system
- Periodically review the effectiveness of the organisation's complaints management system.

Report on complaints

Tasks for implementing the action:

- Review reports on the analysis of complaints data and identify trends and opportunities for improvement
- Define a reporting framework that clearly identifies the data that will be reported on at each level in the service provider
- Provide comprehensive information to the governing body and management about

complaints associated with major risks, and summary information, including trend reports, about all other complaints; this may include:

  - actions taken as a result of a specific complaint or category of complaints
  - indicators such as the time taken to complete actions stemming from complaints

- Disseminate information to the workforce and service users, consumers, carers, families and support people on complaints and their quality improvement implications
- Report complaints to other parties as may be required under legislation (for example, to the Australian Health Practitioner Regulation Agency [Ahpra]) or other obligations (for example, to funders).

Examples of evidence

Examples of evidence may include:

Policy documents that describe the processes for recording, managing, and reporting complaints

A complaints register that includes responses and actions to deal with identified issues, and a schedule for review of these responses

Training documents about the complaints management system

Service user information and resources about the service provider's complaints mechanisms

Feedback from the workforce on the effectiveness of the complaints management system

Feedback from service users and their support people on reported complaints data

Results of audits of compliance with complaints management policies

Evaluation reports that note the effectiveness of responses and improvements in service delivery

Committee and meeting records in which trends in complaints and complaints management are discussed

Reports or briefings on complaints provided to the governing body, the workforce or service users

A quality improvement plan that includes actions to deal with issues identified

Examples of improvement activities that have been implemented and evaluated.

Related actions

This action relates to Action 2.07 (partnerships with service users in governance, planning, design, measurement and evaluation).

Useful resources

1. Toolkit for Health Services. Includes information on involving service users in committees. Available from: http://hic.org.au/toolkit-for-health-services[49]

Diversity and high-risk groups

Action 1.15

The service provider:

a. Identifies the diversity of service users and their support people
b. Identifies groups of service users who are at higher risk of harm
c. Incorporates information on the diversity of service users and their support people, and higher-risk groups, into the planning and delivery of the service.

Intent of the action

The diversity of service users and their support people, and high-risk groups, are considered in the planning and delivery of digital mental health services.

Reflective questions

- What are the sociodemographic characteristics of the service user population and their support people?
- How do these characteristics affect the risk of harm to service users?
- How is this information used to plan service delivery and manage inherent risks for service users and their support people?
- How are the needs of high-risk groups catered for?

Meeting the action

Understanding the characteristics of the service user population allows the service provider to identify groups of service users who may be at greater risk of harm, or who are more likely to have a poor experience of health care because of their condition, age, gender, disability, social, economic or geographic circumstances, cultural background, religion, preferred language, sexuality, or other factors.

Identify the diversity of service users

Tasks for implementing the action:

- Periodically audit the demographic data (such as age, gender, postcode and ethnicity) in the clinical and administrative data systems to find out the diversity of the service users (and, if relevant, their support people) using the digital mental health services
- Use strategic planning processes to consider ways in which the reach of the digital mental health services could be extended to demographic groups not currently accessing the services.

Identify and respond to those at risk of harm

Tasks for implementing the action:

- Analyse relevant data to find out the key risks faced by each demographic group
- Monitor the risk management system and relevant external sources of information (for example, coroners' reports and the published literature) to identify emerging risks affecting groups of service users
- Conduct a risk assessment for groups of service users that are known to be high risk
- Develop strategies to identify high-risk service users, and mechanisms to provide extra safety and quality protections for them and, if relevant, their support people; strategies should be tailored to individual service users – for example, Aboriginal and Torres Strait Islander users will require staff to be trained in the provision of culturally aware and trauma-informed care
- Incorporate service users' risk assessment processes in the quality improvement system if there are specific risks associated with particular types of service users or treatments
- Discuss the strategies to overcome these risks with the clinical governance committee, the workforce, or representatives of the different risk groups
- Ensure that clinical guidelines and pathways for particular conditions or interventions incorporate risk management strategies relevant to known service user risk groups
- Monitor the health outcomes for at-risk service user groups and the actions taken to manage the risks.

Examples of evidence

Examples of evidence may include:

The demographic data for the service provider and its service user communities that are used for strategic planning purposes

The service provider's risk profile, including details of service safety and quality risks, and their potential impact

Results of an assessment or survey of mental health service needs that can be met by digital mental health services

Strategic or business plans that reflect the diversity of the service user population and their support people

Training documents about diversity and cultural awareness

Service user information that is available in formats and languages that reflect the diversity of the service user population

Reports on interpreter use and access (if relevant)

Examples of actions taken to meet the needs of high-risk service users (for example, cultural awareness events).

Related actions

This action relates to Action 1.03 (priorities for diversity) and Action 1.20 (cultural safety).

Healthcare records

Action 1.16

The service provider has healthcare records systems that:

a. Support the creation and maintenance of accurate healthcare records
b. Comply with security and privacy legislation and regulations
c. Support the systematic audit of clinical information and the technical operation of the healthcare record
d. Integrate multiple information systems, where they are used.

Intent of the action

Comprehensive, accurate, integrated, and accessible healthcare records are maintained and available as required.

Reflective questions

- How does the service provider ensure that healthcare records are accurate and integrated (if applicable)?
- How does the service provider ensure the privacy and security of healthcare records?

Meeting the action

Implement an effective healthcare record system

Develop policies, procedures and protocols addressing:

- The recording of clinical information as it is collected
- Standards for documentation, with a focus on the information that should be recorded to enable monitoring of quality of care
- Standards and processes for managing healthcare records, including for:
  - retention
  - digital and manual storage and transport systems
  - access at the point of delivery of digital mental health services
  - emergency access to records when a service user is unable to consent
  - anonymous service users
  - record disposal
- The authorisation of changes to healthcare records
- What information can be extracted for quality assurance, teaching and research purposes (if applicable)
- Compliance with the relevant standards, and with professional and legal requirements
- The conduct of compliance audits.

Structure the healthcare record to guide the clinical and peer workforce to record information important for and relevant to the safety and quality of care.

Employ digital facilities for the reliable and secure management of healthcare records.

Clearly document accountabilities and terms of reference for the individual or committee responsible for governance of the healthcare records system. These accountabilities include the development, review and document control of the forms, documents and files that make up the digital healthcare record (or paper records where still in use).

Implement structures – for example, healthcare record committees – and processes to evaluate healthcare record risks and opportunities and then make changes that will improve the standard of documentation.

Train the workforce

Provide orientation and training to the clinical and peer workforce about the requirements for healthcare record documentation, including the safety and quality rationale for those requirements.

In position descriptions and statements of responsibility for all members of the workforce (clinical and non-clinical), explicitly define the:

- Obligation to protect service user privacy and confidentiality
- Consequences of an intentional breach of the obligation.

Incorporate accountability for healthcare record documentation in performance reviews of the clinical and peer workforce.

Review the healthcare records system

Review the nature and appropriateness of the healthcare records kept for digital mental health services to ensure they are well designed, facilitate documentation of the relevant clinical elements, facilitate clinical audit, and are working effectively.

Review the availability of healthcare records to clinicians and peer workers providing digital mental health care.

Review the processes for maintaining confidentiality and privacy of service user information, including infrastructure, policies, and workforce training for digital mental health service healthcare records, and ensure that they are consistent with the law and good practice.

If multiple information systems are used to capture service user clinical information, periodically review the data systems used with a view to maximising integration.

Audit the system

Periodically audit the design and performance of the healthcare records system and improve the systems, as necessary.

Integration and interoperability

Health-related information can be exchanged electronically among record systems or organisations, with the goal of facilitating access to and retrieval of clinical data by clinicians, peer workers, other healthcare providers, and sometimes by service users.

Determine the policy position on whether the service provider's digital mental health services are to be interoperable with other information systems.

Engage integration and interoperability methodologies to share health-related information seamlessly across geographical, provider, organisational and vendor boundaries, in line with the service provider's policy position on interoperability and with nationally recognised standards.

Examples of evidence

Examples of evidence may include:

Policy documents about healthcare record management, including use, storage, security, consent and sharing of service user information

Results of audits of healthcare records for compliance with policies, procedures, or protocols on healthcare records management, including access to healthcare records and sharing of information

Results of audits of the accuracy, integration, and currency of healthcare records

Committee and meeting records in which the governance of the service provider's data and information technology systems is monitored or discussed

A code of conduct that includes privacy and confidentiality of service user information

Signed workforce confidentiality agreements

Secure digital storage systems

Observations that services are password protected

Records of ethics approvals for research activities that involve sharing service user information

Templates for issuing login and password details for digital healthcare records systems

Results of audits of the use of a unique identifier in the healthcare records management system

Training documents about the healthcare records management system

Systems that enable combining of data from many information systems.

Related actions

This action relates to Actions 1.31 and 1.32 (transparency and consent).

Useful resources

1. Good medical practice: a code of conduct for doctors in Australia. Available at: www.medicalboard.gov.au/Codes-Guidelines-Policies/Code-of-conduct.aspx[50]
2. Guide to health privacy. Available at: www.oaic.gov.au/privacy/guidance-and-advice/guide-to-health-privacy[51]

Action 1.17

The service provider providing clinical information into the My Health Record system has processes that:

a. Optimise the safety and quality of care to service users and their support people
b. Use national patient and provider identifiers
c. Use standard national terminologies
d. Describe access to the system by the workforce, to comply with legislative requirements
e. Maintain the accuracy and completeness of the clinical information the service provider uploads into the system.

Intent of the action

Clinical information shared with the My Health Record system is shared securely in compliance with service users' wishes. Information held in the My Health Record system is accurate, complete, and accessible to authorised persons.

Reflective questions

- Is the information provided to the My Health Record system by the service provider consistent with the legislative requirements of that system?
- If so, what processes does the provider have in place to ensure the accuracy and completeness of clinical information it provides to My Health Record?

Meeting the action

The My Health Record system operates under the *My Health Records Act 2012*.[52] My Health Record allows secure collection, storage, and exchange of health information between healthcare consumers and providers. It uses information from general practitioners, pharmacies, pathology laboratories, imaging services and hospitals to improve the safety and quality of care by supporting the coordination of care and making clinical information accessible in different settings.

Support use of My Health Record

Tasks for implementing the action:

- Develop, maintain, and regularly review organisational policies for using the My Health Record system, and ensure that access follows the requirements of the *My Health Records Act 2012*
- Develop a 'Rule 42 policy' to comply with the *My Health Records Rule 2016* that requires healthcare provider organisations to have, communicate and enforce an access security policy
- Implement physical and technical security measures to control access to the system
- Authorise clinicians to use the system and deactivate accounts of those who no longer need access
- Take reasonable steps to ensure that clinical documents provided to the My Health Record system are accurate at the time of uploading, and that any amendments made to these clinical documents are also uploaded into the system

- Promptly remove any clinical document on the My Health Record system that contains incorrect information; where a clinical document may be subsequently amended or updated (for example, when updated investigation results are provided), upload the corrected version as soon as possible
- Provide training to the workforce about their professional and legal obligations when using the My Health Record system
- Identify and manage system-related security risks
- Regularly review the policy to ensure that it is up to date and in line with any changes to the *My Health Records Act*.

Use unique national healthcare identifiers

Unique healthcare identifiers can prevent duplication of records, minimise the chance of information being assigned to the wrong service user, and help ensure that individuals and clinicians are confident that the correct information is associated with the correct individual at the point of care.

The My Health Record system uses unique national identifiers for patients, clinicians and health service organisations to ensure secure access to healthcare records. Every Australian resident is allocated a unique 16-digit identifier called the Individual Healthcare Identifier. The Australian Health Practitioner Regulation Agency issues unique national identifiers to the clinicians it registers. Health service organisations that employ one or more clinicians can apply for an organisational identifier from the Healthcare Identifiers Service.

Tasks for implementing the action:

- Use unique national identifiers for service users, clinicians, and health service organisations in clinical documents uploaded to the My Health Record system
- Use nationally standardised terms – such as those in the Australian Medicines Terminology – in clinical documents uploaded to the My Health Record system.

Conduct periodic audits

Conduct periodic audits to ensure compliance with the service provider's policies, procedures and protocols for uploading information to, or amending information in, the My Health Record system.

Conduct periodic audits of access to data and records to monitor compliance with legislative requirements.

Examples of evidence

Examples of evidence may include:

Policy documents that describe the service provider's processes for uploading information to the My Health Record system, including the requirement to use national patient and provider identifiers and standard national terminologies

Evidence of information provided by the service provider to the My Health Record system

Results of audits of information provided to the My Health Record system about conformance with the service provider's policy and processes.

Useful resources

1. *My Health Records Act 2012*. Available at: www.legislation.gov.au/Details/C2017C00313[52]
2. e-Health safety (including My Health Record). Available at: www.safetyandquality.gov.au/our-work/e-health-safety[53]
3. Healthcare Identifiers Service – Frequently Asked Questions. Available at: www1.health.gov.au/internet/main/publishing.nsf/Content/pacd-ehealth-consultation-faqs[54]
4. Australian Digital Health Agency. Available at: www.digitalhealth.gov.au[55]
5. My Health Record. Available at: www.oaic.gov.au/privacy/other-legislation/my-health-record[56]
6. Rule 42 guidance. Available at: www.oaic.gov.au/privacy/guidance-and-advice/rule-42-guidance[57]

Criterion: Workforce qualifications and skills

The service provider workforce has the appropriate qualifications, skills, and supervision to ensure the delivery of safe and high-quality care to service users.

Service providers must have strategies in place to manage their workforce. Their systems should ensure excellent leadership and operational processes, a healthy culture, and optimum outcomes for service users. The service provider workforce may directly deliver digital mental health services or support their availability and delivery.

Clinical and technical audits, performance reviews, education and training, compliance with guidelines and a robust model of care can all assist in the provision of safe, high-quality services.

Members of the workforce should:

- Be suitably qualified for the role in which they are engaged
- Only operate within their scope of practice and in line with their skills, experience, and qualifications
- Complete an orientation program that includes the importance of workforce cultural capability
- Complete training in work health and safety
- Complete training in safety and quality in health care
- Attend continuing education and skill enhancement programs applicable to their role.

Several methods are used to confirm and assess the qualifications, experience, professional standing, and other relevant professional attributes of the workforce. These include recruitment processes, registration checks, peer review, oversight and supervision, and competency assessment.

Defining the scope of practice of a clinician or peer worker involves delineating the extent of their practice within the organisation based on their credentials, competence, performance and professional suitability, and the needs and capability of the service provider.

Performance development programs enable an organisation to ensure that members of its workforce meet their continuing professional development and professional registration requirements, where these apply. Issues affecting an individual's performance are identified and addressed as part of the performance development process. Goals for quality improvement, and further education and training, are also agreed to.

The values of fairness, accountability and support underpin effective systems of performance development. If underperformance is identified, the first response that is triggered should include increased support, and access to relevant tools, education, and expertise. However, service user safety is paramount, and remedial strategies should always protect the safety of service users.

Orientation is an important activity that provides the workforce with the basic knowledge and skills to work safely. Comprehensive orientation for the workforce providing or supporting digital mental health services includes an introduction to the service provider's:

- Digital mental health service(s) and their model(s) of care
- Service values and requirements – for example, non-stigmatising, trauma-informed, person-centred, recovery-orientated services

- Policies, procedures and protocols
- Risk reporting and risk management processes
- Quality assurance, improvement, and monitoring systems
- Incident management and investigation systems
- Feedback and complaints management systems
- Healthcare records systems
- Performance development and human resources systems
- Information technology systems.

Service providers should support their workforce to use the best available evidence to provide safe, high-quality care. Good clinical governance promotes clinical practice that is effective and based on evidence.[17] Likewise, good technical governance supports the provision of secure and stable systems for the delivery of high-quality care.

Members of the workforce are accountable for their practice. This includes compliance with accepted guidelines or pathways and the documented model of care.

Supervision as well as wellbeing programs and Employee Assistance Program (EAP) support are important investments in the delivery of high-quality care. They provide opportunities for skills development and may improve practice safety. They also help to ensure members of the workforce receive the support they require to fulfil their roles. For the peer workforce, access to lived-experience supervisors with knowledge and experience of peer practice is strongly recommended.

Safety and quality training

Action 1.18

The service provider provides orientation to the organisation that describes roles and responsibilities for the safety and quality of services for:

a. Members of the governing body

b. Clinicians, peer workers, technicians, and other members of the workforce.

Intent of the action

Members of the governing body and the workforce understand the approach to, and their roles and responsibilities for, safe and high-quality digital mental health services.

Reflective questions

- What information is provided to new members of the governing body and the workforce about their roles and responsibilities for the safety and quality of services?

Meeting the action

Orientation introduces a member of the governing body or the workforce to the organisation. A well-designed orientation program will detail the key safety and quality systems and the governance of the service.

Several tasks are important for implementing the action.

Review the service provider's orientation policies and programs in conjunction with the governing body and the workforce. Consider whether they provide appropriate and effective orientation to the safety and quality of digital mental health services and to clinical and technical governance for all members of the workforce, including contracted, student and volunteer members.

Provide orientation that covers the essential elements of clinical and technical governance and quality improvement systems. This will set expectations for members of the governing body and the workforce, and help maintain and develop their competence and expertise in safety and quality.

Periodically evaluate the content of the orientation and induction training program for its effectiveness and currency of content.

Examples of evidence

Examples of evidence may include:

Orientation and induction documents that detail the safety and quality roles and responsibilities of the workforce and the governing body

Attendance records for orientation and induction training

Reports on evaluation of orientation and induction training content.

Related actions

This action relates to Action 1.24 (roles and responsibilities).

Note: Although the responsibility to assign safety and quality roles and responsibilities to the workforce is set out in Action 1.24, Action 1.18 ensures orientation about their roles and responsibilities for safety and quality is delivered to members of the governing body and the workforce.

Action 1.19

The service provider uses its training systems to:

a. Assess the competency and training needs of its workforce
b. Implement a training program to meet its requirements arising from these standards
c. Provide access to training to meet its safety and quality training needs
d. Monitor the workforce's participation in training.

Intent of the action

The workforce is appropriately trained to meet the need of the service provider to provide safe and high-quality digital mental health care.

Reflective questions

- How does the service provider assess the skill levels of members of the workforce, identify gaps and mediate them?
- What training does the service provider provide about safety and quality?
- How does the service provider identify workforce training needs to ensure that workforce skills are current and meet the service provider's service delivery requirements?

Meeting the action

Service providers have a responsibility to provide access to ongoing education and training to maintain a competent and capable workforce. Training can be provided internally or externally using various formats, including:

- Face-to-face programs
- Short sessions
- Peer review
- Mentoring and supervised practice
- Self-directed programs
- Online learning modules
- Audio and video content
- Competency-based assessments
- Conferences and seminars
- Secondments and placements.

Provide leadership for training

Tasks for implementing the action:

- Define mandatory education and training requirements for all members of the workforce in relevant aspects of safety, quality, leadership, and clinical and technical risk
- Review the service provider's education and training policies and programs and consider whether they provide regular, appropriate and effective education and training in safety and quality and clinical and technical governance
- Provide each member of the workforce with the opportunity, through performance review and development programs, to define their education and training goals and agree with their manager on opportunities to achieve these goals, in line with the service provider's objectives and priorities and service user needs
- Support the provision of education and training to the workforce based on a comprehensive and regularly updated assessment of need, the competencies required for their roles, and the need to meet the requirements of the NSQDMH Standards
- Regularly assess the training needs of the workforce – for example, via professional development activities, training gap analysis, analysis of incident management and investigation systems, and workforce surveys
- Maintain records of relevant education and training undertaken by each member of the workforce to ensure that the workforce maintains skills and competencies
- Evaluate the outcomes of education and training provided to the workforce.

Examples of evidence

Examples of evidence may include:

Policy documents about orientation and training of the workforce

Employment records that detail the skills and competencies required of each position, as well as the safety and quality roles and responsibilities

Evidence of assessment of the workforce's needs for education and competency-based training

A schedule of workforce education and competency-based training that includes the requirements of the NSQDMH Standards

Orientation manuals, education resources or records of attendance at workforce training

Results of audits of the proportion of the workforce with completed performance reviews

Skills appraisals and records of competencies for the workforce

Feedback from the workforce about their training needs

Reviews and evaluation reports of education and training programs

Communication to the workforce about annual training requirements.

Action 1.20

The service provider has strategies to provide culturally safe services to meet the needs of its Aboriginal and Torres Strait Islander service users and their support people.

Intent of the action

Digital mental health services are culturally safe and meet the needs of Aboriginal and Torres Strait Islander service users and their support people.

Reflective questions

- What strategies does the service provider have to provide culturally safe services that meet the needs of its Aboriginal and Torres Strait Islander service users and their support people?

Meeting the action

Cultural awareness is a basic understanding that there is diversity in cultures across the population. Cultural competency extends beyond individual skills or knowledge to influence the way that a system or services operate across cultures. It is a process that requires ongoing learning. One-off training does not create a culturally competent workforce but could increase cultural awareness. A culturally safe workforce considers power relations, cultural differences and the rights of the patient, and encourages workers to reflect on their own attitudes and beliefs. Cultural respect is achieved when individuals feel safe and cultural differences are respected.[12,23]

Cultural safety is determined by Aboriginal and Torres Strait Islander individuals, families, and communities.[13,18] Aboriginal and Torres Strait Islander peoples do not always experience mainstream health services as offering them a safe and secure place to get well. Factors that contribute to a poor experience include isolation from community and kin, language barriers, financial difficulties in gaining access to treatments, and inferior treatment.[11,22]

Improve the cultural safety of the service provider and the workforce

Service providers must take active steps to ensure that their digital mental health services are culturally safe.

Tasks for implementing the action:

- Establish partnerships with Aboriginal and Torres Strait Islander peoples and community-controlled organisations, and collaborate with them to improve the cultural safety, cultural respect and cultural competence of the service provider and its workforce
- Define cultural respect and cultural safety and the principles that underpin them, including:
  - leadership
  - health equality and a human rights approach
  - community and consumer engagement
  - partnerships
  - monitoring and accountability
  - an ongoing commitment to learning, education and training
- Incorporate cultural safety into policy development
- Provide leadership that shows an ongoing commitment to self-determination of, and equality and partnership with, Aboriginal and Torres Strait Islander peoples, and fosters a safe digital environment that

supports the rights and dignity of Aboriginal and Torres Strait Islander service users and their support people

- Review the service provider's education and training policies and programs to ensure that they adequately cover cultural safety, cultural respect and cultural competency and monitor workforce participation in training
- Include cultural safety, cultural respect, and cultural competency as part of performance review processes, and provide access to ongoing learning for individuals through training, professional development, critical reflection, and practice improvement
- Ensure that actions to improve cultural safety are implemented and monitored for effectiveness.

Improve the cultural safety of the digital mental health services

Tasks for implementing the action:

- In collaboration with Aboriginal and Torres Strait Islander partners, review the cultural safety of the digital mental health services currently offered, including their language, content, usability and accessibility
- Based on this review, consider how to improve the cultural safety of the digital mental health services
- Ensure that the roles, responsibilities, and accountabilities for providing culturally safe digital mental health services are clearly articulated
- Collaborate with Aboriginal and Torres Strait Islander peoples to inform digital mental health service governance, planning, design, measurement and evaluation
- Incorporate cultural safety into the specifications for the development of digital mental health services.

Monitoring and reporting on cultural safety

Tasks for implementing the action:

- Seek feedback from Aboriginal and Torres Strait Islander service users and their support people about the cultural safety of digital mental health services
- Monitor and report on cultural safety to the governing body and management.

Cultural safety for other diverse population groups

Although this action specifically requires strategies to meet the needs of Aboriginal and Torres Strait Islander service users and their support people, it highlights an opportunity for service providers to consider the cultural needs of other population groups. Within the context of their budget and resources, service providers can set priorities for actions to meet the diversity of needs of those from culturally and linguistically diverse backgrounds.

Examples of evidence

Examples of evidence may include:

A policy document that outlines the service provider's approach to cultural safety, including strategies and training to improve cultural safety, cultural respect, and cultural competency

Communication to the workforce about cultural safety, cultural respect, and cultural competence

Records of attendance at cultural safety training

Skills appraisal and records of competencies for the workforce in cultural safety, cultural respect, and cultural competence

Feedback from service users who identify as Aboriginal and Torres Strait Islander about their experience of the cultural safety of the services.

Related actions

This action relates to Action 1.03 (priorities for diversity) and Action 1.15 (diversity).

Useful resources

1. NSQHS Standards User Guide for Aboriginal and Torres Strait Islander. Available at: www.safetyandquality.gov.au/publications-and-resources/resource-library/nsqhs-standards-user-guide-aboriginal-and-torres-strait-islander-health[22]
2. Cultural Respect Framework 2016–2026 for Aboriginal and Torres Strait Islander Health: A national approach to building a culturally respectful health system. Available at: www.coaghealthcouncil.gov.au/Portals/0/National%20Cultural%20Respect%20Framework%20for%20Aboriginal%20and%20Torres%20Strait%20Islander%20Health%202016_2026_2.pdf[23]
3. Engaging with Indigenous Australia – exploring the conditions for effective relationships with Aboriginal and Torres Strait Islander communities. Available at: www.aihw.gov.au/reports/indigenous-australians/engaging-with-indigenous-australia-exploring-the/summary[58]
4. Cultural safety in health care for Indigenous Australians: monitoring framework. Available at: www.aihw.gov.au/reports/indigenous-australians/cultural-safety-health-care-framework/contents/background-material[59]
5. Cultural competency in the delivery of health services for Indigenous people. Available at: www.aihw.gov.au/getmedia/4f8276f5-e467-442e-a9ef-80b8c010c690/ctgc-ip13.pdf.aspx[60]
6. Improving care for Aboriginal and Torres Strait Islander patients resource kit. Available at: www.health.vic.gov.au/publications/improving-care-for-aboriginal-and-torres-strait-islander-patients-resource-kit[61]
7. Map of Indigenous Australia. Available at: https://aiatsis.gov.au/explore/map-indigenous-australia[62]

Performance management

Action 1.21

The service provider has valid and reliable performance review processes that:

a. Require members of the workforce to regularly take part in a review of their performance
b. Identify needs for training and development in safety and quality
c. Incorporate information on training requirements into training systems.

Intent of the action

The service provider routinely reviews and discusses individuals' performance, and systematically collects information on individuals' safety and quality training needs.

Reflective questions

- What are the service provider's performance review processes?
- What processes are used to identify the training needs for each member of the workforce?
- How is this information incorporated into the service provider's training systems?

Meeting the action

Performance review and performance development are the systematic processes of goal-setting and periodic one-on-one review of workforce performance. Performance review processes present an opportunity for managers and their workforce to clarify reciprocal obligations between the service provider and the workforce.

The service provider is responsible for:

- Establishing a culture in which safe, high-quality care can be delivered
- Assisting members of the workforce to develop their competence and performance by supporting them to achieve agreed goals.

Members of the workforce are responsible for:

- Understanding the service provider's priorities and objectives
- Setting professional goals that are consistent with the service provider's objectives
- Working collaboratively with the service provider to achieve professional and organisational goals.

Develop an effective system

Many tasks can assist with meeting this action. For example, ensure the performance review and development system includes:

- Setting and clarifying expectations for the workforce
- Monitoring workforce performance
- Planning and reviewing workforce performance
- Developing workforce capability
- Recognising workforce achievements
- Resolving unsatisfactory workforce performance.

Set out a performance review and development policy that includes:

- The role of performance review in supporting the safety and quality of digital mental health services
- How performance review can support reflective practice and provide opportunities for the workforce to identify areas for improvement
- Processes for periodic performance review of the workforce and the requirements for their participation in formal audit, peer review and continuing professional development
- How the skills of the clinical, peer worker and technical workforce will be assessed when competency-based assessment and training are required
- Processes for identification of individual training needs
- The support, resources, training, and access to evidence-based tools and data on their performance that will be provided to the workforce and how time will be allocated to support their practice.

Implement performance review processes for clinicians, peer workers, technicians, and other members of the workforce.

Develop review processes for members of the workforce who are employed indirectly through contract arrangements. This may include reviewing performance data when contracts are due for renewal or addressing feedback and issues as they are identified.

Periodically conduct a training needs analysis and use this to inform the review of the training system.

Monitor and review the system

Tasks for implementing the action:

- Identify one or more designated persons who are responsible for ensuring compliance with the service provider's performance development policy
- Monitor and report on performance and training to support effective implementation of the performance development system
- Review the effectiveness of the performance development system, including workforce participation and actions to respond to training and development needs.

Examples of evidence

Examples of evidence may include:

Policy documents about the performance review process for the workforce
Documented performance development systems that meet professional development guidelines and credentialing requirements
Results of audits of the proportion of the workforce with completed performance reviews, including actions taken to deliver identified training and development needs
Mentoring or peer-review reports
Feedback from the workforce about their training needs
Review and evaluation reports about education and training
Committee and meeting records in which performance review and credentialing of clinicians are discussed.

Qualified workforce

Action 1.22

The service provider has processes to ensure clinicians and peer workers involved in the design and delivery of services:

a. Have the necessary skills, experience, and qualifications for these roles

b. Have, and work within, a defined scope of clinical practice.

Intent of the action

Clinicians and peer workers are appropriately skilled and experienced to perform their roles safely, and to provide services within an agreed scope of practice.

Reflective questions

- What processes are used to ensure that clinicians and peer workers have the appropriate qualifications, experience, professional standing, competencies, and other relevant professional attributes?
- What processes are used to ensure that clinicians and peer workers are working within the agreed scope of practice when designing services or providing care to service users?
- How does the service provider match the services provided with the skills and capability of the workforce?

Meeting the action

Define scope of clinical practice

Allowing for service needs, organisational capability and the digital mental health services provided, service providers should appoint clinicians and peer workers who are suitably experienced, skilled, and qualified to practise in a competent and ethical manner.

While the term 'scope of clinical practice' is used in the NSQDMH Standards, for peer workers this should be read as 'scope of practice' – it is acknowledged that peer workers do not deliver clinical services.

Tasks for implementing the action:

- Clearly define the scope of practice of clinicians and peer workers in the context of the digital mental health services delivered
- Include the scope of practice in position descriptions and contracts for workers' services
- Establish effective processes for reviewing clinicians' and peer workers' competence and performance
- Set out expectations about the supervision of clinicians and peer workers, if relevant
- Regularly review clinicians' and peer workers' scope of practice
- Confirm procedures to be followed if a concern arises about the capability of a clinician or peer worker
- Develop processes for the safe and appropriate introduction of new digital mental health services, including the expectations and requirements for clinicians and peer workers.

Collect evidence of credentials

Clearly set out the minimum credentials to be verified as part of any recruitment process – for example:

- Education, qualifications and formal training
- Previous experience, including activity and experience in settings similar to the relevant scope of practice
- References and referee checks
- Continuing education that relates to the role in which the clinician or peer worker is engaged and that is relevant to their scope of practice
- Current registration with the relevant national board, if applicable
- Professional indemnity insurance, if applicable
- Other documentation and pre-employment checks, such as:
  - a current curriculum vitae
  - an applicant's declaration
  - proof of identity (100-point identity check)
  - passport and copies of relevant visas (for overseas-trained practitioners)
  - a police or working with children check.

Establish the process for submission and review of supporting documents, including certification by a Justice of the Peace or similar recognised certifying agent, as required.

Verify the information submitted by, or on behalf of, a clinician or peer worker for determining scope of practice, including information received from recruitment agencies.

Maintaining scope of practice

Tasks for implementing the action:

- Regularly conduct credentialing processes to review the scope of practice for all clinicians and peer workers and report on the credentialing processes to the governing body
- Consider any added support, supervision or training that may be required by clinicians and peer workers to ensure that their practices are safe
- Reconsider clinician's and peer worker's scope of practice when there is a change in circumstances or a change in role for them
- Periodically review whether the process for defining scope of practice is appropriately designed, resourced, maintained and monitored
- Incorporate periodic review of the process for defining scope of practice into audit programs, with a focus on consistency with adopted standards, performance measures and outcomes.

Examples of evidence

Examples of evidence may include:

Policy documents about the scope of clinical practice for clinicians and peer workers in the context of the service provider's needs and capability and the digital mental health services delivered
Committee and meeting documents that include information on the roles, responsibilities, accountabilities and monitoring of scope of clinical practice for the clinical and peer workforces
Results of audits of position descriptions, duty statements and employment contracts against the requirements and recommendations of clinical practice and professional guidelines
Reports of key performance indicators for clinicians and peer workers
Workforce performance appraisal and feedback records that show a review of the scope of clinical practice for the clinical and peer workforces
Peer-review reports
Evaluation of the service provider's clinical services targets
Procedure manuals or guidelines for new digital mental health services

Defined competency standards for new digital mental health services
Planning documents for introduction of new digital mental health services (including consideration of workforce, equipment, procedures and scope of clinical practice)
Training documents about new digital mental health services
Communication to the workforce that defines the scope of clinical practice for new digital mental health services.

Related actions

This action relates to Action 2.09 (partnering with service users and their support people to incorporate their views and experience into the training and education for the workforce).

Useful resources

1. Standard for Credentialling and Defining the Scope of Clinical Practice. Available at: www.safetyandquality.gov.au/sites/default/files/migrated/credentl1.pdf[63]
2. Peer workforce role in mental health and suicide prevention. Available at: www.health.gov.au/resources/publications/primary-health-networks-phn-mental-health-care-guidance-peer-workforce-role-in-mental-health-and-suicide-prevention[64]

Action 1.23

The service provider has a process to ensure technicians involved in the design and delivery of services have the necessary skills, experience and qualifications for this role.

Intent of the action

Technicians are appropriately skilled and experienced to perform their roles safely.

Reflective questions

- What processes are used to ensure that technicians have the appropriate qualifications, experience, professional standing, competencies, and other relevant professional attributes?
- What processes are used to ensure that technicians are working within the agreed scope of their expertise when designing or supporting services?
- How does the service provider match the services provided with the skills and capability of the technical workforce?

Meeting the action

When technicians supporting digital mental health services are suitably experienced, trained, and qualified, user safety is improved.

Tasks for implementing the action:

- Clearly define the roles and responsibilities in position descriptions and contracts for all technicians, including for those with independent decision-making authority and those working under supervision
- Establish processes to regularly review the roles of technicians and report outcomes to the governing body
- Reconsider technicians' roles when there is a change in the service provider's digital mental health service
- Incorporate periodic review of processes for defining the role of technicians into audit programs, with a focus on consistency with adopted standards, performance measures and outcomes.

Examples of evidence

Examples of evidence may include:

Policy documents that describe the formal processes for selecting and appointing or contracting the technical workforce

A register of technical workforce qualifications and areas of expertise

Documented recruitment and procurement processes that ensure that technicians are matched to positions, and have the required skills, experience, and qualifications to perform their roles and responsibilities

Employment and contract documents that define the roles of technical supervisors

Evidence that the service provider has verified technicians' qualifications before employment

Documented performance reviews or peer reviews for the technical workforce.

Safety and quality roles and responsibilities

Action 1.24

The service provider has processes to:

a. Assign safety and quality roles and responsibilities for services to the workforce

b. Support the workforce to understand and perform their roles and responsibilities for safety and quality.

Intent of the action

Every member of the workforce understands and enacts their roles and responsibilities for the safety and quality of digital mental health services.

Reflective questions

- How are members of the workforce informed about, and supported to fulfil, their roles and responsibilities for safety and quality?

Meeting the action

Tasks for implementing the action:

- Review the organisational structure, position descriptions and contract templates of management, clinicians, peer workers, technicians, and other members of the workforce to ensure that responsibility for safety and quality is clearly defined at all levels
- Review the educational programs for the workforce to ensure that it includes training in clinical and technical governance and foundational safety and quality elements, including:
  - risk from the service user's perspective
  - clinical and technical governance responsibilities for safety and quality
  - legislative responsibilities related to service user harm and reportable incidents
  - incident investigation methods
  - principles of teamwork and leadership style
  - open disclosure
  - creating and sustaining a safety culture that is based on person-centred care
- Discuss safety and quality responsibilities in routine performance management processes and identify professional development opportunities in safety and quality, leadership, and risk.

Examples of evidence

Examples of evidence may include:

Policy documents that outline the delegated safety and quality roles and responsibilities of the workforce

Employment documents or contracts that describe the safety and quality roles, responsibilities, and accountabilities of the workforce

An organisational chart and delegations policy that show clinical and technical governance reporting lines and relationships

Training documents about safety and quality roles and responsibilities of the workforce

Communication to the workforce about their safety and quality roles and responsibilities

Performance appraisals that include feedback to the workforce about delegated safety and quality roles and responsibilities

Results of workforce surveys or feedback regarding their safety and quality roles and responsibilities.

Related actions

This action relates to Action 1.18 (orientation).

Note: Although the responsibility to assign safety and quality roles and responsibilities to the workforce is set out in Action 1.24, Action 1.18 ensures orientation about those roles and responsibilities is delivered to members of the governing body and the workforce.

Criterion: Safe environment for the delivery of care

The environment promotes safe and high-quality care for service users.

The service provider should consider how their environment can support the delivery of safe and high-quality care for service users. The service provider environment – which includes digital systems and infrastructure as well as physical facilities, plant, and equipment – must be fit for purpose and maintained in good working order to reduce hazards and ensure service safety.

A safe environment for the delivery of care also requires the environment to be culturally safe with the provision of wellbeing and EAP support measures that enable workers to care for themselves and others.

In the digital environment there are several points that are dealt with by the actions in this criterion, including:

- The terms and conditions for use of a digital mental health service
- The risk of abuse, exploitation or loss of dignity resulting from engaging in a digital mental health service, especially for children and young people
- The ethical, professional and legal restrictions on the way information about an individual's mental health and wellbeing can be used
- The collection, use, disclosure, storage, transmission, retention, and destruction of service user data
- Information security management systems.

Safe environment

Action 1.25

The service provider maximises the safety and quality of care:

a. Through the design of services, the digital operating systems and internal access controls
b. By ensuring the terms and conditions for use of services are fair and transparent and do not mislead service users and, where relevant, their support people
c. By ensuring devices and other infrastructure are fit for purpose and well maintained
d. By developing and using processes for the prompt implementation of legislative and regulatory changes.

Intent of the action

The digital and physical environments support safe and high-quality digital mental health care appropriate to the service user's needs. The terms and conditions for the service user to engage with the digital mental health service are transparent and support safe care.

Reflective questions

- How does the service provider ensure that the design of the environment supports the quality of care provided to service users?
- How does the service provider ensure that devices and infrastructure are safe and maintained in good working order?
- How does the service provider assess their terms and conditions to ensure they are fair and transparent and do not mislead service users?

Meeting the action

A safe environment for the delivery of digital mental health services requires consideration of a variety of factors, including the:

- Characteristics of the digital service and environment
- Physical environment from which the service is delivered
- Context and location of the service user receiving the service.

Tasks for implementing the action:

- Reflect Australian standards for devices and equipment in the organisation's policies and procedures, so that purchases, repairs, and replacements are carried out following a specified standard
- Clarify expectations about the manufacturers' guidelines for the use and tolerances of equipment and devices
- Maintain a record of all devices, equipment, and plant – including, as a minimum, the date of purchase, preventive maintenance schedule, location, and serial number
- Implement a comprehensive maintenance plan and a schedule of review to ensure that all devices and infrastructure are regularly maintained and fit for purpose

- Clearly document all routine and preventive maintenance, repairs, patches, and upgrades
- Regularly test equipment to ensure its readiness – including servers, generators, and battery backups – and maintain records of dates of testing
- Regularly conduct audits to see whether the digital environment is safe and promotes best practice
- Maintain a register of legislative and regulatory changes that have been applied to digital mental health services each year, and document the actions taken by the service provider in response to the changes.

Service user environment

The service provider should consider any aspect of the physical environment of the service user that may contribute to making use of the digital mental health service unsafe. Train the workforce to consider and respond to these aspects, including:

- Lack of privacy in the user environment
- The possibility of domestic violence
- A young person who is in out-of-home care and only has intermittent access to their appointed guardian.

Terms and conditions

Terms and conditions of use may be incorporated into end-user licence agreements or terms of use. When agreeing to the terms and conditions of a digital mental health service, when fees are charged or the service user provides some other kind of consideration, the service provider and user are effectively entering into a contract which sets out the rights and responsibilities of each party.[65] It is unlawful for businesses to force or coerce anyone into entering into a contract, or induce them to enter into a contract by using false or misleading information.

Service users may have a variety of rights and remedies under consumer laws. Service providers must ensure:

- Their terms and conditions of use are fair and transparent
- That service users properly understand the nature of the services they will receive, how their information will be used, and the kind and amount of any fees involved in using the services
- That the services being provided are safe and suitable for the intended users, or variety of users, and are provided as promised by the service provider.

Research has indicated that many consumers do not read terms and conditions because they are too long, difficult to comprehend, difficult to find, or because users perceive the cost of reading to outweigh the benefits.[66]

Tasks for implementing the action:

- Review the terms and conditions for digital mental health services to ensure that they are fair, easy to read, clear, transparent, written in appropriate language and do not mislead the potential service user
- Consider providing a short summary of the terms and conditions so the service user can understand them quickly and easily
- Audit compliance with applicable consumer law.

Examples of evidence

Examples of evidence may include:

Policy documents that describe the service provider's:

- requirements for maintaining devices and infrastructure
- reporting lines and accountability for actions, including during emergency situations

A strategic plan for digital assets, devices, and infrastructure

A maintenance schedule for devices and infrastructure

Results of audits of compliance with maintenance schedules and inspections of digital devices and infrastructure

Results of audits of the use of a pre-purchase checklist and risk assessment to identify suitability of all new digital devices and infrastructure.

Related actions

This action relates to Action 1.28 (privacy), and Action 2.10 (usability).

Action 1.26

The service provider has systems to:

a. Minimise risk of abuse of service users and, where relevant, their support people
b. Minimise risk of exploitation of service users and, where relevant, their support people
c. Preserve the dignity of service users and, where relevant, their support people.

Intent of the action

Aspects of the digital mental health service environment that can increase risks of harm from abuse and exploitation are identified and managed, and steps are taken to ensure the dignity of service users is maintained.

Reflective questions

- What systems are in place to prevent the abuse and exploitation of service users?

Meeting the action

Abuse may be in the form of discrimination, cyberbullying, harassment, trolling, stalking, threats, defamation, or image-based abuse. Abuse may be sexist, misogynistic, racist, homophobic or transphobic. A digital mental health service failing to provide an appropriate treatment, intervention or response, may also be perceived by some as a form of abuse.

Exploitation through digital services may occur through scams, hidden costs, inappropriate advertising or in-product sales, or blackmail – such as demands for money, intimate images, or sexual favours.

A loss of dignity can occur from malicious actions like using fake accounts, impersonation, doxing (when personal details are shared or publicised online) and swatting (when an abuser makes a hoax call to emergency services in an attempt to get a large number of police or emergency service responders to go to an address). A loss of dignity may also result from inappropriate language, poor service design, or implementation issues causing delays in accessing treatment, frustration, or damage to confidence and self-esteem.

Abuse, exploitation, and loss of dignity can add burdens for people who are already experiencing mental health concerns or stress.

Tasks for implementing the action:

- Collaborate with service users, consumers, carers, families, and their support people to better understand what comprises abuse, exploitation, and loss of dignity in digital mental health services; use this to inform policy and service development
- Develop a policy and procedures on how to incorporate, enhance and assess user safety throughout the design, development, and deployment of the service provider's digital mental health services

- Prioritise the use of trauma-informed practice in digital mental health services; use a strengths-based approach, based on understanding and responding to the impacts of trauma, to enhance the physical, psychological, and emotional safety of both providers and service users – this will maximise opportunities for recovery
- Conduct a risk assessment to identify where there is a high risk of abuse, exploitation, or loss of dignity for service users when using digital mental health services; develop strategies to manage the identified risks
- Identify ways for service users and their support people to report abuse, exploitation or loss of dignity that they have experienced while using digital mental health services.

Australia's eSafety Commissioner has developed Safety by Design Principles[67], which provides tips for service users on how to protect their personal information and gives direct links for reporting abuse. Service providers may choose to refer to this information or make it available to their service users.

Examples of evidence

Examples of evidence may include:

Policy documents that describe the service provider's requirements to prevent abuse and exploitation of service users in the digital environment and to protect their dignity

Checklists and contract specifications for services that outline the requirements to prevent abuse and exploitation of service users and to protect their dignity

Information resources for service users about prevention from abuse and exploitation and protection of dignity

Results of audits of services – that is, systems to prevent abuse and exploitation

Analysis of incidents, complaints, and feedback data from service users about abuse, exploitation and loss of dignity in the digital environment, and any actions taken to remedy that.

Useful resources

1. Trauma-informed care and practice. Available at: mhcc.org.au/publication/trauma-informed-care-and-practice-ticp[68]
2. Safety by Design principles. Available at: www.esafety.gov.au/about-us/safety-by-design[67]
3. The eSafety Guide. Available at: www.esafety.gov.au/key-issues/esafety-guide[69]

Action 1.27

The service provider has systems to minimise the risk for children and young people to be harmed while using a service.

Intent of the action

Aspects of the digital mental health service environment that can increase risks of harm to children and young people are identified and managed.

Reflective questions

- How does the service provider ensure that the design of services supports the safety of children and young people?
- What processes are in place to protect the safety of children and young people?

Meeting the action

Children and young people are at risk of all the forms of abuse and exploitation associated with digital technology (as listed in Action 1.26). Issues specific to this age group include the risks of grooming, unwanted contact, online hate, catfishing, trolling, inappropriate photo sharing, and cyberbullying. Spending too much time online may also represent a risk for the wellbeing of children and young people.

The service provider must not place the burden of safety solely on the service user. They must take steps to ensure that the digital mental health services they make available to children and young people do not facilitate, inflame, or encourage illegal and inappropriate behaviours.

The National Principles for Child Safe Organisations have been developed to drive implementation of a child-safe culture across all sectors providing services to children and young people. This is to ensure the safety and wellbeing of children and young people across Australia.[70]

Make safety of children and young people a priority

Tasks for implementing the action:

- Set out in a policy document the requirements for a child-safe environment and for the delivery of services that align with the National Principles for Child Safe Organisations, and have it endorsed by the governing body
- Conduct a gap analysis against the National Principles for Child Safe Organisations to identify areas for improvement and inform the development of an action plan

- Establish a dedicated role that requires specific knowledge of child safety issues and has responsibility for the safety of children and young people using the service provider's digital mental health services
- Provide a single point of contact for children, young people, carers, families, and support people who are seeking advice or support regarding the safety or wellbeing of children and young people
- Endorse a child safety reporting procedure that nominates the position that is to be informed about all reports of incidents or risks involving the safety of children and young people
- Ensure that a consistent response occurs to any incidents or risks that involve the safety of children and young people
- Review the service provider's digital mental health services for exposure to threats, risks, problems or content that is triggering, harmful or inappropriate for children and young people; develop strategies to manage identified risks
- Ensure privacy settings for digital mental health services are comprehensive and set at the highest levels of protection by default.

Support service users

Tasks for implementing the action:

- Ensure service users are aware of and can use safety features – this will increase understanding, confidence and trust in digital mental health services
- Identify ways for children and young people, or their support people, to report harm or potential harm they have experienced
- Ensure appropriate authentication and consent processes are in place before digital mental health services can be accessed by children and young people, including when parental agreement is required before a service can be accessed by a child
- Encourage adult supervision of a child or young person using a digital mental health service
- Promote the eSafety Guide developed by Australia's eSafety Commissioner; it contains tips for a service user on how to protect their personal information and block someone, and provides direct links to report abuse
- Establish guidelines for service users for online groups or forums, outlining the preferred way of interacting
- Engage trained human moderators to help create a safe environment for young people engaging in online groups or forums.

Examples of evidence

Examples of evidence may include:

Policy documents that describe the service provider's:

  - requirements for ensuring that children and young people are protected from harm and exploitation
  - reporting lines and accountability for actions to protect children and young people from harm, abuse and exploitation

Results of audits of compliance with policies that minimise the risk of harm to children and young people

Observations of the design and use of interventions that reduce risks relating to potential harm to children and young people

Analysis of incident reports relating to harm to children and young people, and action taken to deal with issues identified

A risk register and quality improvement plan that includes information from an analysis of incidents relating to harm to children and young people.

Related actions

This action relates to Action 1.11 (incident management), Action 1.13 (feedback) and Action 1.14 (complaints management).

Useful resources

1. National Principles for Child Safe Organisations. Available at: https://childsafe.humanrights.gov.au/national-principles[70]
2. Safety by Design principles. Available at: www.esafety.gov.au/about-us/safety-by-design[67]
3. The eSafety Guide. Available at: www.esafety.gov.au/key-issues/esafety-guide[69]
4. ThinkUKnow: Preventing online child sexual exploitation. Available at: www.thinkuknow.org.au[71]

Privacy

Action 1.28

The service provider conducts a privacy impact assessment for each service in accordance with best practice.

Intent of the action

The impact of a digital mental health service on privacy rights and legislative obligations is assessed, and risks to the privacy of a service user are managed, minimised, or eliminated.

Reflective questions

- Has the service provider conducted a privacy impact assessment that identifies and manages privacy risks of each service?
- What processes are in place to assess the security of the service and protect the privacy of service users?

Meeting the action

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 privacy impact assessment is a tool for identifying and assessing privacy risks throughout the development lifecycle of a program or system. It involves a systematic assessment to identify the impact that a digital mental health service might have on the privacy of service users, and sets out recommendations for managing, minimising, or eliminating that impact.[72] It should also consider whether the planned uses of personal information in the service will be acceptable to the community.

In the Guide to undertaking privacy impact assessments, the Office of the Australian Information Commissioner describes the steps in a privacy impact assessment process, including conducting a threshold assessment to find out whether any more steps are necessary.

Establish the policy and process

Tasks for implementing the action:

- Endorse a policy and an agreed process for conducting privacy impact assessments – for example, by using a nominated privacy impact assessment template
- Include in the policy the key elements to be delivered by the privacy impact assessment, including:
  - describing how personal information flows within the service
  - analysing the possible impacts on service user privacy
  - identifying and recommending options for avoiding, minimising or mitigating negative privacy impacts
  - building privacy into the design of the service
  - achieving the service's goals while minimising negative and enhancing positive privacy impacts.
- Review project management and risk management policies and procedures to ensure that they incorporate the conduct of a privacy impact assessment for digital mental health services.

Undertake a privacy impact assessment

Tasks for implementing the action:

- Provide training for staff about conducting a privacy impact assessment
- Conduct a threshold assessment for each of the service provider's digital mental health services to find out if a privacy impact assessment is required
- Use the service provider's endorsed template to complete a privacy impact assessment for each relevant digital mental health service
- Ensure that privacy risks identified through a privacy impact assessment are included on the risk register and that actions are taken to manage, mitigate or eliminate the risks.

Review the privacy impact assessment

Tasks for implementing the action:

- Regularly review the digital mental health services, noting those which have had significant updates or changes, and find out whether those services need updated privacy impact assessments
- Update or conduct a new privacy impact assessment when there are substantial changes to how personal information will be handled.

Examples of evidence

Examples of evidence may include:

A completed privacy impact assessment for each service

Committee meetings in which the results of the privacy impact assessments are discussed

A register of actions taken to remedy issues identified by the privacy impact assessments

Observation that the design of the service aligns with the privacy impact assessments.

Useful resources

1. Guide to undertaking a privacy impact assessment. Available at: www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments[72]
2. Privacy impact assessment tool. Available at: https://www.oaic.gov.au/privacy/guidance-and-advice/privacy-impact-assessment-tool[73]
3. Privacy impact assessment eLearning course. Available at: https://education.oaic.gov.au/elearning/pia/welcome.html[74]
4. Threshold assessment template. Available at: www.oaic.gov.au/privacy/guidance-and-advice/when-do-agencies-need-to-conduct-a-privacy-impact-assessment[75]
5. Privacy impact assessments (including template and guide). Available at: https://ovic.vic.gov.au/privacy/privacy-impact-assessment[76]
6. Privacy Impact Assessment Toolkit (New Zealand). Available at: www.privacy.org.nz/publications/guidance-resources/privacy-impact-assessment[77]
7. The Five Safes framework. Available at: www.aihw.gov.au/about-our-data/data-governance/the-five-safes-framework[78]

Action 1.29

The service provider has privacy policies for each service that are:

a. Easy to understand and transparent for service users and their support people
b. Uphold service users' rights and choices
c. Readily available to service users and their support people before accessing and while using the services
d. Compliant with privacy laws, privacy principles and best practice.

Intent of the action

Each digital mental health service has a readily available privacy policy that meets the needs of service users.

Reflective questions

- Does each service have an up-to-date privacy policy?
- Are these privacy policies easy to find and easy to understand for service users?
- Does the privacy policy protect service users' privacy rights and give them the choices expected to protect their rights?

Meeting the action

Understanding privacy requirements

The privacy policy of a digital mental health service is a statement that explains in simple language how the service collects, handles, stores, uses and discloses personal information, including sensitive information. It explicitly describes whether and when that information is kept confidential or is shared with or sold to third parties.

Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable. Sensitive information includes health information, and it generally has a higher level of privacy protection than other personal information.

The confidentiality of most health information is protected by statutory and common law requirements of confidentiality and privacy. However, the legislative requirements may vary between states and territories, between Australian Government entities and state and territory entities, and because of other factors, including the location of the collecting entity.

Service providers should review the Australian Privacy Principles and other relevant Commonwealth, state and territory privacy and health records laws and principles to shape the relevant requirements for their digital mental health services.

Research has indicated that many consumers do not read privacy policies because they are too long, difficult to comprehend, difficult to find, or because users perceive the costs of reading outweigh the benefits.[66]

Tasks for implementing the action:

- Implement systems and processes to comply with all legislative requirements for privacy and confidentiality that apply to the service provider's digital mental health services
- Endorse a process for the development of a privacy policy that is readily accessible, easy to understand, transparent, up to date, and compliant with privacy laws, privacy

principles and best practice for each of the service provider's digital mental health services
- Conduct an audit of the service provider's existing digital mental health services and ensure that each service has a privacy policy that aligns with this process
- Recognise the role of service user consent in the use or disclosure of information for purposes other than direct provision of care (see Actions 1.31 and 1.32)
- Provide appropriate digital infrastructure to aid in ensuring service user's privacy
- Understand the interaction between My Health Record legislative requirements and privacy legislative requirements.

Implementing and maintaining privacy policies

Tasks for implementing the action:

- Review the specifications for the development of new digital mental health services and ensure that the need for a privacy policy is included
- Regularly review incidents, service user complaints and feedback from service users that relate to privacy and confidentiality, and take action to deal with any issues
- Set up a mechanism to ensure that relevant policies and procedures are updated to reflect any changes to privacy legislation, principles and regulations
- Conduct training for the workforce on privacy and confidentiality, and acknowledge the impact that the culture and practices of the workforce have on the protection of service user personal information.

Examples of evidence

Examples of evidence may include:

Policy or contract documents that describe the service provider's requirements for the privacy policy of a service, ensuring that service users' privacy is protected
Results of audits of compliance of services with privacy policy requirements
Observation of privacy policies of services
Feedback from service users on the ease of access to privacy policies and the ease of understanding and transparency
Analysis of incident reports about the compliance of services with privacy laws, privacy principles and best practice
A risk register and quality improvement plan that includes information from an analysis of incidents relating to privacy policy of services.

Related actions

This action relates to Action 1.31 (transparency of data collection and use).

Useful resources

1. Australian Privacy Principles. Available at: www.oaic.gov.au/privacy/australian-privacy-principles[79]
2. Guide to developing an APP privacy policy. Available at: www.oaic.gov.au/privacy/guidance-and-advice/guide-to-developing-an-app-privacy-policy[80]
3. Open and transparent management of personal information. Available at: www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-1-app-1-open-and-transparent-management-of-personal-information[81]

Action 1.30

The service provider advises service users and, where relevant, their support people of change to privacy policies in a timely and comprehensible way.

Intent of the action

Service users and, where relevant, their support people are informed when the privacy policy of a digital mental health service they currently use changes.

Reflective questions

- How does the service provider monitor the need for changes to the privacy policies of its services?
- What processes are in place to advise service users of changes to privacy policies?

Meeting the action

A privacy policy for a digital mental health service should be a living document that is subject to regular reviews and updates. It should remain up to date with the service's data practices and meet the latest legal requirements.

Process for providing updates

Tasks for implementing the action:

- Include a requirement in relevant policies and procedures to advise service users and, where relevant, their support people of any substantial or material change to a privacy policy
- Specify the format to be used for notifications
- Allocate clear roles and responsibilities for notifying service users of the change
- Set up a mechanism to record changes to the privacy policies of the service provider's digital mental health services, including details of the nature and extent of the changes, and actions taken; file previous versions
- Periodically conduct an audit of existing digital mental health services to review whether there have been changes to privacy policies and whether all service users were advised in line with the policy.

Communicating updates to the privacy policy

Tasks for implementing the action:

- Provide privacy policy update notices to service users in one or more ways to maximise transparency – for example, by email or by using a pop-up notice on the service provider's website
- Include in the privacy policy update notice:
  - the effective date of the updated privacy policy
  - details of the most important changes
  - what to do if a service user does not accept the changes
  - information on how to view the updated privacy policy
- Implement a process to re-obtain consent when there has been a substantial or material change to the privacy policy
- Seek feedback from service users on their experience of the notification of change; use this information to inform future update practices
- Review complaints and incidents that relate to changes to the privacy policy of a digital mental health service and use this information to guide future updates.

Examples of evidence

Examples of evidence may include:

Policy document that describes the service provider's requirement that service users be advised of changes to privacy policies in a timely way

Contracts with services that specify timely notification to the service provider of changes to privacy policies

Results of audits of compliance with the policy requirement to notify service users of a change in privacy policy

Information provided to service users about changes in privacy policy

Analysis of complaints from service users about a failure to be advised of a change in the privacy policy of a service.

Useful resources

1. What is a privacy policy? Available at: www.oaic.gov.au/privacy/your-privacy-rights/what-is-a-privacy-policy[82]
2. Guide to developing an APP privacy policy. Available at: www.oaic.gov.au/privacy/guidance-and-advice/guide-to-developing-an-app-privacy-policy[80]

Transparency

Action 1.31

The service provider has systems for the collection, use, disclosure, storage, transmission, retention, and destruction of data that provide service users and, where relevant, their support people with:

a. Information on the types of data collected and how the information is used
b. Information on any interoperable healthcare services
c. Information on who has access to their data, including through data sharing agreements, provision or sale to third parties, and if transfer of data outside Australia occurs
d. Timely information if requests to access data by external parties are granted by the service provider
e. Protection of their data that was provided anonymously or using a pseudonym
f. Prevention against the unauthorised re-identification of anonymous or de-identified data
g. Notification if the service ceases operation or changes ownership
h. Information on where their data will go if the service ceases to operate or changes ownership
i. Information on the legacy of their data.

Intent of the action

Appropriate systems are in place to manage data, and the use of data is transparent to service users.

Reflective questions

- What systems are in place for the collection, use, disclosure, storage, transmission, retention, and destruction of data?
- How are service users informed about the types of data collected and how the information is used?
- Is the service user made aware of who has access to their data?
- What processes are in place to inform service users when requests to get their data are granted?
- What processes are in place to protect service users who use services anonymously?
- How is the re-identification of data prevented?
- How does the service provider manage service user legacy data?

Meeting the action

Service users should know that their sensitive personal information is safe, and that it will only be used for the purposes for which it was provided and by the people or organisation it was provided to. Service providers should take a proactive and transparent approach to the safe collection and storage of service user data.

Keep track of information

Service users have the right to know:

- What information service providers collect through their digital mental health services
- How that information is stored and used (with their consent), including when information is shared with technology providers or business analytic services for improving the service
- What rights and choices they have about the collection, use and disclosure of their personal information.

Tasks for implementing the action:

- Endorse a policy that outlines the service provider's collection, use, disclosure, storage, transmission, retention, and destruction of data, throughout their digital mental health services; it must consider:
  - management of data from anonymous users or those using a pseudonym
  - de-identification of data
  - management of data if a digital mental health service ceases operation or changes ownership
  - management of data if a service user dies
- Implement robust processes for what, and how, information will be made available to service users and, if relevant, their support people. This information may be about:
  - the types of data collected (including service users who have accessed a digital mental health service anonymously or by using a pseudonym)
  - how service user data are used
  - data sharing for any reason, including via data sharing agreements or requests by external parties
  - the provision or sale of data to third parties
  - whether service user data are transferred outside of Australia
  - the management of data if a digital mental health service ceases operation or changes ownership or if a service user dies
- Include information on data collection, use, disclosure, storage, transmission, retention and destruction in the product information that is made available to potential service users of each digital mental health service (see Action 3.03)
- Review the systems and processes for the collection, use, disclosure, storage, transmission, retention, and destruction of data for digital mental health services to ensure that they meet legislative and regulatory requirements and service user expectations, and support the strategies and priorities articulated in the service provider's strategic and operational plans.

Manage expectations

Re-identification of individuals from data that have been de-identified (in compliance with legal obligations) can occur.[83,84] Service users may have concerns about being identified from sensitive personal data shared with third parties, even when the data are anonymised. They may also hold fears that their mental health information could be accessed by others without their knowledge or consent.

Tasks for implementing the action:

- Provide service users and their support people with a clear explanation of how their information is collected, used, disclosed, stored, transmitted, retained and destroyed, and the safeguards that apply
- Write terms and conditions and privacy policies in simple language that is easy to understand; ensure that the service user can choose between different types of uses and sharing
- Maintain appropriate data sharing agreements
- Make explicit to service users when data are stored or transferred out of Australia.

Interoperable healthcare services

Interoperability is a complex concept. At its simplest, it is the ability to move or share information easily between people, organisations, and systems, while ensuring that its meaning is preserved from one context to another so

that the information is interpreted consistently when it is moved or shared.[85]

A lack of interoperability between systems or services may contribute to disjointed care, incidents, inefficiencies, and poor-quality data.[85] For this reason, interoperability is seen by many as a desirable goal for digital health services and there has been considerable effort directed towards increasing interoperability in Australia.

The NSQDMH Standards do not require digital mental health services to be interoperable. However, when services are interoperable the service user must be made aware of the services with which their data and information are being shared, and consent to the information sharing, as required by privacy legislation and best practice.

Service providers should maintain a record of all services that are interoperable with the service provider's digital mental health services, regularly update the record, and provide information on interoperable services to service users and, if relevant, their support people.

Requests by external parties

Service providers may receive requests from third parties for information on, or a comprehensive record of, a specified service user. Service user consent is required for the release of personal information in response to a request by a third party, except when disclosure of their information is required or permitted by law or by legislative requirements such as a subpoena.

Tasks for implementing the action:

- Develop guidelines and flowcharts to inform decisions about the release of information, and clearly state when service user consent is required in different circumstances, for example:
  - under legislative requirements
  - when requested by a third party
  - when a transfer of care occurs
- To help provide transparency and build trust, outline processes for how and when service users are to be informed that third-party access has been granted.

Data breaches

A data breach occurs when there is unauthorised access to, or disclosure of, information, or when information is lost in circumstances in which such unauthorised access or disclosure is likely to occur. The *Privacy Amendment (Notifiable Data Breaches) Act 2017* establishes a mandatory data breach notification scheme in Australia. It requires businesses covered by the Privacy Act to notify any individuals affected by a data breach that is likely to result in serious harm.

Data breaches can occur in several ways, including:

- Loss or theft of devices or records containing personal information
- Disposal or return to suppliers of hard-disk drives and digital storage media without the contents first being erased
- Hacking of databases or otherwise illegally accessed
- Workers accessing or disclosing personal information outside the requirements or authorisation of their employment
- Mistakenly providing personal information to the wrong person, for example, while providing health care
- An individual deceiving a service into improperly releasing the personal information of another person.[86]

Tasks for implementing the action:

- Develop guidelines, possibly including a flowchart, that detail the actions required in response to a data breach, along with clear roles and responsibilities for managing the associated process
- Advise individuals affected by a data breach – note that this is a legislated requirement in some circumstances.

Anonymity, pseudonymity, de-identification and re-identification of data

Some digital mental health services allow service users to make use of services anonymously or by using a pseudonym. Anonymity and pseudonymity are important privacy concepts, because they enable service users to exercise greater control over their personal information, and decide how much personal information will be shared with others.

Anonymisation may provide for the safe use or sharing of data within an organisation, or be used to produce aggregated information, whereas pseudonymisation produces anonymised data but on an individual-level basis.

Whenever de-identified or pseudonymised data are used, there is a residual risk of re-identification. For example, data matching or similar techniques may allow anonymised or de-identified data to be turned back into identifiable personal data.

When implementing this action, develop robust data governance processes to protect service users' privacy whenever a service provider uses or releases de-identified or pseudonymised data. This includes:

- Ensuring that the digital mental health service's privacy policy clearly explains the approach to, and potential consequences of, the anonymisation or de-identification of data
- Ensuring that there is clear accountability for de-identification within the service provider
- Building and ensuring ongoing transparency around their de-identification practices
- Ensuring that those who undertake de-identification have adequate and up-to-date training, and if need be ensuring appropriate external expertise is sought
- Conducting ongoing and regular re-identification risk assessments to check that methods used remain effective at, and appropriate for, managing the risks involved
- Establishing a plan to deal with any re-identification attacks or events
- Auditing data recipients to ensure that they are complying with the conditions of any data sharing agreements
- Considering new information that becomes available, and whether any such information increases re-identification risk.

When a service ceases operation or changes ownership

The need for service providers to safeguard personal information is not waived when a digital mental health service ceases operation or a previous system is retired, or when ownership of the service changes.

Tasks for implementing the action:

- Establish clear guidelines that outline how service user data will be managed if a digital mental health service is retired, ceases to operate, or ownership is transferred to another service provider
- Establish arrangements to inform service users of these changes and seek consent when required
- Ensure that service user consent is obtained before transfer of their digital mental health service records to a new service provider
- Arrange suitable storage when service user records will not be transferred to another service provider and ensure that the records can be accessed if required.

Legacy data

Legacy data may arise when ceasing a service, retiring a previous system or when a service user dies. A service user's right to confidentiality does not end when they are deceased.

Tasks for implementing the action:

- Establish a legacy data management plan that includes arrangements for archiving longer-term data efficiently and securely
- Develop a process to ensure consent to get a deceased service user's mental health records is requested from the executor or administrator of their estate, or from

another specified party, in line with the applicable legislative provisions.

Training

Conduct training for the workforce on the systems and processes for the collection, use, disclosure, storage, transmission, retention, and destruction of data for digital mental health services.

Monitor and review

Tasks for implementing the action:

- Conduct regular audits to assess compliance with the policy on the collection, use, disclosure, storage, transmission, retention, and destruction of data, and take action to remedy issues identified
- Conduct regular audits to check whether information provided to service users and, if relevant, their support people agrees with the service provider's documented processes, and take action to remedy issues identified
- Ensure that data and information risks identified through these audits are included on the risk register and that actions are taken to manage, mitigate or eliminate the risks
- Ensure that service users and their support people are aware of ways to provide feedback about the collection, use, disclosure, storage, transmission, retention and destruction of data for digital mental health services
- Regularly review complaints and incidents that relate to the collection, use, disclosure, storage, transmission, retention, and destruction of data for digital mental health services, and take action to remedy any issues identified
- Develop and implement specific policies and procedures about the use of personal information for clinical, educational, quality assurance and research purposes; include robust authorising procedures for any uses or disclosures outside the usual provision of care.

Examples of evidence

Examples of evidence may include:

Policy documents that describe the service provider's requirement to inform service users about the collection, use, disclosure, storage, transmission, retention, and destruction of data

Product information that includes details about the information collected and who will have access to the service user's data

Results of audits of compliance with the policy requirements for data collection, use and sharing

Communication to service users about the data collected, how it is used and who has access to it

Analysis of incident reports relating to how data are collected, used, disclosed, stored, transmitted, retained or destroyed

Committee or meeting records in which the collection, use, disclosure, storage, transmission, retention or destruction of data are discussed, and actions taken to remedy any issues

Communication to service users about the granting of a request by a third party to use their data

Policy documents that describe the service provider's duty to protect the anonymity of service users when requested

Policy documents that describe the service provider's duty to prevent the re-identification of anonymous or de-identified data

Analysis of complaints by service users about the anonymity of their data not being protected.

Related actions

This action relates to Action 1.11 (incident management), Action 1.12 (risk management), Action 1.29 (privacy), and Action 1.35 (security and stability).

Useful resources

1. *Privacy Act 1988*. Available at: www.legislation.gov.au/Series/C2004A03712[87]
2. Australian Privacy Principles. Available at: www.oaic.gov.au/privacy/australian-privacy-principles[79]
3. Guide to Data Analytics and the Australian Privacy Principles. Available at: www.oaic.gov.au/privacy/guidance-and-advice/guide-to-data-analytics-and-the-australian-privacy-principles[88]
4. De-identification Decision-Making Framework. Available at: www.oaic.gov.au/privacy/guidance-and-advice/de-identification-decision-making-framework[89]
5. Anonymisation: managing data protection risk code of practice (UK). Available at: https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf[90]
6. Data breach preparation and response. Available at: www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response[91]
7. Australian Privacy Principles Guidelines, Chapter 5: APP 5 – Notification of the collection of personal information. Available at: www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-5-app-5-notification-of-the-collection-of-personal-information[92]

Action 1.32

The service provider has mechanisms for service users to:

a. Consent to the use of personal data and records for any purpose beyond direct care
b. Consent before any personal data and records are used in research, unless they are de-identified
c. Withdraw or withhold consent for the collection, storage or distribution of their personal data and records
d. Opt out from the sharing of their personal data and records
e. Access, copy and amend their personal data and records
f. Request deletion of their personal data and records.

Intent of the action

Service users have control of how their data are collected, stored, distributed and used.

Reflective questions

- How does the service provider get consent from service users for the use of their data for any purpose beyond direct care?
- Does the service provider have processes to de-identify data that are used in research?
- Does the service provider offer service users the opportunity to opt out of data sharing?
- What processes are in place for service users to view and copy their data or to request for them to be deleted?

Meeting the action

Seeking consent

Service user consent to the use of personal data and records may be expressed verbally, in writing or by conduct implying consent. The format of the consent should be informed by the nature, complexity and level of risk of the digital mental health service and the service user data and records collected and kept.

Consent to the collection, storage or distribution of personal data and records for purposes other than direct care must be able to be withheld or withdrawn without adverse implications for the service user's access to the digital mental health services. Any approach that requires agreement to data handling terms and conditions in order to use a service is not providing true 'informed consent', because it does not offer service users choice, protection or opportunity for redress.

Tasks for implementing the action:

- Conduct a risk assessment to inform the level and form of consent required to use service user data and records for any purpose beyond direct care
- Adopt a comprehensive policy and associated procedures on informed consent by service users regarding the use of personal data and records, including:
  - how consent is obtained
  - when consent is implied
  - when consent is required
  - when consent is not required
  - how data and records from service users are distributed or used

  - how service users can withdraw or withhold consent for the collection, storage or distribution of their personal data and records
  - how service users can opt out of sharing of personal data and records
  - how service users can view, copy and amend their personal data and records
  - how service users can request deletion of their personal data and records
- Review current informed consent processes for existing digital mental health services to ensure that they align with the policy and procedures, and take any corrective action necessary
- If the service provider seeks consent for their data handling practices in the terms and conditions of their digital mental health service, ensure that these terms include an undertaking to handle data as described in the privacy policy of the digital mental health service, relevant legislation and professional ethics
- Link informed consent on personal data and records to the service provider's open disclosure policy and national, state or territory consent policies (if applicable)
- Establish a process for service users to negotiate the privacy terms outlined by the digital mental health service, including the option to opt out of sharing their personal data and records
- Alternatively, provide service users with genuine choice about the use of their data by specifying categories of data use to which they can give informed consent – such as 'data used only to deliver the service', 'data shared or sold to third parties' and 'data used to assess eligibility or exclusion for products and services'
- Implement consent that requires renewal after specified expiry dates to ensure that the consent reflects changes in user preferences over time.

When consent is not required

Consent to the use of personal data and records for a purpose beyond direct care may not be required in certain circumstances – for example:

- When disclosure is required or authorised by or under an Australian law or court or tribunal order
- When disclosure is part of normal internal business practices, such as auditing or business planning, or when only de-identified data are shared.

Consent to the use of data and information for quality assurance or evaluation of a service is also generally exempt from consent requirements.

If information has been appropriately de-identified, it is no longer considered personal information. It can therefore be used or shared in ways that would otherwise require the consent of the service user. Care must be exercised when de-identifying personal information to ensure that it cannot be re-identified (see Action 1.31).

To implement this action, establish a process that informs service users whenever their personal data and records may be shared or used without their consent under the Australian Privacy Principles. Include all the people or entities to which information may be disclosed in this way, and any functions or activities of the service provider that involve personal information and are contracted out (e.g. business analysis).

Develop a policy that provides guidance to the workforce on quality assurance and evaluation, including consent, privacy, relevant legislation, national and professional standards and when ethical review is required.

Consent for use of personal data and records in research

The National Statement on Ethical Conduct in Human Research (2007)[93] is published by the National Health and Medical Research Council and was updated in 2018. It consists of a series of guidelines that follow the *National Health and Medical Research Council Act 1992* and includes information on the health research privacy framework.

Consent to the use of data for research can be:

- Specific – related to a specific project
- Extended – for use in future research that is an extension of a current project or in the same general area of research
- Unspecified – for use in any future project.

Tasks for implementing the action:

- Establish a process to clearly explain to potential research participants the terms and implications of their consent to the use of their data for research
- Ensure that service users considering participation in research are provided with the opportunity to ask questions and discuss the information about the research and their decision with others
- Clearly record consent provided by a service user for the use of their personal data and records in research.

View, copy and amend

Service users have a right to request access to their personal information and to request its correction if they believe it is inaccurate, incomplete, out of date or misleading. They may also request a copy of their personal information. Service providers must provide a service user access to their personal information upon request, except when the law allows them to refuse the request. Service users do not have a right to get other kinds of information from the service provider, such as commercial information.[79]

A service provider can refuse to give access to a service user's health information in some situations – such as if:

- It may threaten the service user's or someone else's life, health or safety
- It may impact someone else's privacy
- Giving access would be unlawful.[79]

If giving a service user certain information would affect someone else's privacy, a service provider can block out that part and give the service user the rest of the information. If information cannot be given directly to the service user because of a concern for their health or safety, then access may be given through an agreed third party.

Rights to obtain and correct personal information under privacy legislation operate alongside, and do not replace, other informal or legal procedures by which an individual can be provided with access to, or correction of, their personal information – for example the *Freedom of Information Act*.

Tasks for implementing the action:

- Develop a policy and procedure to show service users how to get or correct their personal information and records; include indicative response times, access charges, how access is to be given, and the provisions if access is refused
- Provide service users access to their personal information and records in a manner that is as prompt, uncomplicated and inexpensive as possible
- Make the policy widely available on the service provider's website or in the privacy policy for the digital mental health service
- Develop a form for service users to request to access or correct their personal information and records (note that a service user cannot be required to use a particular form to make an access or correction request)
- Regularly review the procedure for service users to access or correct their personal information to ensure that it is flexible and facilitates rather than hinders access.

Requesting deletion

Service users may, on occasion, request that their personal data be deleted. This is sometimes referred to as 'data erasure' or 'the right to be forgotten'. Some personal health data may be subject to a legal requirement to maintain it for a minimum specified period, meaning it cannot be deleted, despite the request of a service user.

Tasks for implementing the action:

- Include in the data handling policy the nature of the personal information the service provider holds on service users and whether, and in what circumstances, it can be deleted
- Document the procedure to be followed when a request to delete data is made by a service user, including:
  - review of the personal data that the service provider holds on the service user
  - deletion of the service user's data unless there is a valid reason to refuse – for example, a legal, regulatory or other requirement
  - ascertaining whether personal data may have been distributed to other parties and, if possible, telling those parties about the request for data deletion.

Educate the workforce

Support informed consent for the collection, storage, distribution and sharing of personal data and records by educating and training of the workforce in:

- Effective communication to underpin good practice
- The legal, ethical, and practical foundations of requirements for service user personal data and records consent
- The service provider's personal data and records consent policy and procedures
- The barriers to understanding during the consent process – for example, individual health and digital literacy levels and the health literacy environment.

Monitor and review

Schedule periodic reviews of the effectiveness and outcomes of the policy on informed consent for use of personal data and records, and take action to deal with any issues identified.

Regularly review service user feedback, complaints and incidents that relate to informed consent for the collection, use, distribution and sharing of personal data and records for digital mental health services, and take action to deal with any issues identified.

Examples of evidence

Examples of evidence may include:

A policy document that

- describes the service provider's need for service users to consent to their personal data and records being used for any purpose beyond direct care
- provides service users with the option to opt out from sharing personal data and records
- allows service users to view and copy their personal data and records
- allows service users to request deletion of their personal data and records

A policy document outlining requirements for the de-identification of personal data and records that are used in research

Consent forms for service users to consent to personal data and records being used

Observation of processes to allow service users to opt out of sharing their personal data and records

Procedures about how to respond to requests to view, copy or delete personal data and records

Analysis of incident reports relating to the use of personal data and records without consent

Notifications to service users when deletion of personal data is complete.

Related actions

This action relates to Action 1.25 (terms and conditions), Action 1.31 (transparency of data handling), and Action 2.02 (informed consent).

Useful resources

1. Australian Privacy Principles. Available at: www.oaic.gov.au/privacy/australian-privacy-principles[79]
2. Australian Privacy Principles Guidelines: Key concepts. Available at: www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-b-key-concepts[94]
3. National Statement on Ethical Conduct in Human Research. Available at: www.nhmrc.gov.au/file/9131/download?token=4Qw7LMvh[93]
4. Ethics in quality assurance and evaluation activities. Available at: www.nhmrc.gov.au/about-us/resources/ethical-considerations-quality-assurance-and-evaluation-activities[95]
5. APP Guidelines Chapter 3: APP 3 – Collection of solicited personal information. Available at: www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-3-app-3-collection-of-solicited-personal-information[96]

Costs and advertising

Action 1.33

The service provider provides service users and, where relevant, their support people with clear and transparent information on the:

a. Direct costs to access the service

b. Estimated data usage requirements for using the service.

Intent of the action

The service user is fully informed of the direct costs associated with using a digital mental health service and the foreseeable indirect contributors to cost.

Reflective questions

- How does the service provider inform service users about the costs and data requirements for using its services?

Meeting the action

The direct costs of a digital mental health service include any up-front and ongoing fees to use the service, such as purchase of an app, in-app fees, a monthly subscription fee, and the cost per session.

Indirect costs could include internet, call or data usage charges, and will vary depending on several factors, including the type of digital service, the service user's location, their internet or mobile phone plan, the technology the service user is using, the data requirements of the digital mental health service, and the service user's level of use of the service. While it may not be possible to give an accurate indication of indirect costs, enough information should be provided to allow for an indicative cost to be estimated – for example, average data requirements for each contact with the digital mental health service. Optional in-app purchases are another form of indirect cost about which there should be transparency.

Develop a policy

Tasks for implementing the action:

- Endorse a policy document that includes the pricing principles and other factors when estimating the cost of a digital mental health service to service users; include direct and indirect costs, conditions of access, and refunds
- Ensure that this policy aligns with the endorsed strategic priorities of the service provider
- Include in the policy the process for informing potential service users about the costs of accessing and using a digital mental health service and a demand for the information to be clearly set out, in simple and easy-to-understand language that takes account of the different health and digital literacy levels of service users
- Collaborate with service users, consumers, carers, families, and support people to inform the pricing of digital mental health services and consider how information on service costs is best presented to potential users
- Provide information about the costs of a digital mental health service through product information, via a website, at point of first contact or via the terms and conditions of a service.

Review current information

Tasks for implementing the action:

- Regularly review the terms and conditions and product information of all existing digital mental health services to ensure that the direct and indirect costs of accessing and using the service are clearly set out, easy to understand, up to date, and not misleading, and take action to remedy any identified issues
- Review feedback and complaints from service users about direct and indirect costs of digital mental health services and use this information to revise the policy on pricing and communication.

Engage with service users

Tasks for implementing the action:

- Engage with service users, consumers, carers, families and support people to better understand the impact of direct and indirect costs on access to, and use of, the service, and how to best present information about the direct and indirect costs of accessing and using a service to potential service users
- Provide information on direct and indirect costs to potential service users via the product information developed for each digital mental health service (see Action 3.03)
- Periodically seek feedback from service users about the clarity of the information provided to them on the direct and indirect costs for using the digital mental health service; use this information to improve the provision of information.

Related actions

This action relates to Action 1.25 (safe environment – terms and conditions).

Examples of evidence

Examples of evidence may include:

Policy documents about providing information about the costs and data requirements of using services to users
Communication to service users about the costs and data requirements
Observation of information provided to service users about costs and data requirements of using services
Analysis of feedback and complaints from service users about costs or data requirements
Survey of service users about the information provided about costs and data requirements of the services
Product information statements.

Useful resources

1. In-app purchases. Available at: www.accc.gov.au/consumers/mobile-phone-services/in-app-purchases[97]

Action 1.34

The service provider ensures that in-product sales or advertising:

a. Complies with Australian Consumer Law and regulatory requirements
b. Is appropriate for service users.

Intent of the action

In-product sales or advertising do not mislead, exploit, or disadvantage service users.

Reflective questions

- Do the service provider's services use in-product sales or advertising?
- How does the service provider review legal and regulatory requirements about in-product sales or advertising?
- What processes are in place to ensure that any in-product sales or advertising is appropriate for the intended users of its services?

Meeting the action

In-product sales or advertising can, in theory, occur in any digital mental health service, although it is most common in mobile health applications.

Understand the issues

In-product sales and advertising in digital mental health services pose a risk to service users who may be unduly influenced and not exercise appropriate judgement. Service users may be in a vulnerable mental state when accessing a digital mental health service, or may have implicit trust and confidence in advertising provided by their treating service.

A conflict of interest may arise if the service provider is receiving financial benefit from the in-product sales or advertising. An undisclosed financial interest may conflict with their duty to provide independent diagnosis, advice, and treatment. To overcome this conflict of interest, the service provider must disclose the known benefits and risks of the marketed product(s) and the nature of their financial interests in the product(s).

The Medical Board of Australia's *Good medical practice: a code of conduct for doctors in Australia*[50] includes sections specifically about conflicts of interest and financial transparency, and requires doctors to declare any financial interest in products endorsed by or sold from their practice, and to not make an unjustifiable profit thereby. As a result, health professionals who are involved with a service provider that offers in-product marketing without appropriate and full disclosure may be at risk of a breach of their ethical and professional obligations.[98]

The Psychology Code of Ethics contains sections focused on how to safeguard the best interests of all parties to the psychological service and how to avoid financial arrangements that may adversely influence the psychological services provided, whether at the time of provision or subsequently.[99]

While all registered health professionals must comply with a profession-specific code of conduct or code of ethics, non-registered healthcare workers should also meet prescribed standards for practice and conduct, as set out in the National Code of Conduct for health care workers.[101]

A service provider should:

- Establish a comprehensive policy on in-product sales and advertising for digital mental health services that includes:
  - whether in-product sales or advertising will be permitted
  - how the appropriateness of the product(s) being sold or advertised is assessed, taking into account the intended users of the digital mental health service and the service provider's ethical framework (this includes products being sold or advertised through online advertising platforms)
  - provision for declaration of conflicts of interest
  - compliance with legislative and regulatory requirements
  - how the policy is monitored
- Implement procedures for declaring real or perceived conflicts of interest to service users
- Conduct regular audits of the volume and nature of in-product sales and advertising that have been delivered in conjunction with the service provider's digital mental health services to assess whether they comply with the endorsed policy; take action to deal with any issues identified
- Regularly review service user complaints and incidents that relate to in-product sales and advertising for digital mental health services, and use this information to update the policy and improve processes.

Examples of evidence

Examples of evidence may include:

Policy documents about in-product advertising and sales

Audit results that show conformance with policy requirements

Analysis of feedback or complaints relating to the inclusion of advertising or sales within services

Guidelines about how to decide what might be considered appropriate advertising for service user groups

Observation of the information provided to service users on in-product sales and advertising.

Useful resources

1. Australian Consumer Law. Available at: https://consumerlaw.gov.au/australian-consumer-law[99]
2. Good Medical Practice: A code of conduct for doctors in Australia. Available at: www.medicalboard.gov.au/Codes-Guidelines-Policies/Code-of-conduct.aspx[50]
3. Australian Psychological Society Code of Ethics. Available at: https://psychology.org.au/about-us/what-we-do/ethics-and-practice-standards/aps-code-of-ethics[100]
4. National Code of Conduct for health care workers. Available at: www.coaghealthcouncil.gov.au/NationalCodeof ConductForHealthCareWorkers[101]

Security and stability

Action 1.35

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.

Intent of the action

An information security management system is in place that protects the security and stability of digital mental health services.

Reflective questions

- Does the service provider have information security management systems in place?
- Does it take a risk-based approach to information security management?
- Are the roles and responsibilities for information security management clear?

Meeting the action

Make information security a priority

Information security is about providing confidentiality, integrity, and availability by protecting information from unauthorised user access, data modification and removal.

It therefore deals with information assets and the protection of data from any form of threat.

The terms cybersecurity and information security are often used interchangeably but cybersecurity is one form of information security – one that focuses on protecting data in cyberspace from cyber attacks. Cybersecurity threats can include software attacks (viruses, worms, trojan horses, bots, adware, spyware, ransomware, scareware, rootkits, zombies), theft of intellectual property, identity theft, theft of equipment or information, sabotage and information extortion.

Information security must be paramount for service providers that hold many types of valuable information, including sensitive health information, especially given the risks associated with a data breach and the increasingly sophisticated modes of violation.[102] Healthcare is a very lucrative target for cybercriminals because of the value and quantity of personal data held.[103]

To meet this action, the governing body must show leadership of and commitment to an information security management system by:

- Establishing information security as a documented priority
- Endorsing an information security management policy
- Supporting the information security management system through allocation of appropriate budgets and resources
- Receiving regular reports on information security management.

It is also important to conduct an information security risk assessment that includes identification and evaluation of the information assets of the service provider, such as:

- Computers, phones and physical data storage media
- Servers – both physical and virtual
- Network infrastructure
- Cloud services
- Service user information
- Other assets, including data on paper.

This information can contribute to a risk analysis to identify risks related to the potential loss of information.

Implement an information security management system

An information security management system is a structured and systematic approach to managing information security and other IT-related risks. It includes wide-ranging controls to keep data secure from diverse security threats. It can help to assure general information security, as well as personal data protection.

Security controls may encompass organisational structures, people, roles, policies, processes, procedures, instructions, training, guides, and IT systems, including:

- Information security policies
- Organisation of information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- Systems acquisition, development, and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management
- Compliance.

Tasks for implementing the action:

- Establish an information security management system that is based on an information security risk assessment; include security controls that reflect the critical and sensitive nature of the information assets, and the processes and assessed needs of the service provider
- Develop and endorse a policy and associated procedures to support the maintenance and operation of the information security management system, including:
  - assigning information security roles, responsibilities, and authorities
  - outlining the process to identify, analyse and treat information security risks
- Ensure that the information security management system is informed by all information security incidents (actual and near miss), including data breaches and technical faults, and that it incorporates continuous feedback and improvement activities that deal with changes in the threats, vulnerabilities and impacts of information security incidents
- Allocate enough resources and budget to maintain an information security capability that reflects the business and regulatory needs of the service provider and the size and extent of threats to its information assets
- Conduct training and education for the governing body and the workforce about the information security management policy; ensure that those with delegated information security roles and responsibilities are competent in those roles.

Monitor and maintain the information security management system

Tasks for implementing the action:

- Routinely monitor, measure, analyse and evaluate the performance (efficiency and effectiveness) of the information security management controls, including undertaking systematic testing; make systematic improvements when required
- Periodically audit the service provider's compliance with the endorsed information security management system and all associated improvement processes, and take action as required to deal with the findings of the audit
- Regularly report on the performance of the information security management system to the governing body and to the workforce
- Benchmark the service provider's security practices against established standards
- Seek certification of the information security management system by an accredited certification body.

The ISO 27000-series[104] comprises information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission. ISO 27001 provides a structured methodology dedicated to information security and the requirements for an information security management system.

The Australian Cyber Security Centre (ACSC) leads the Australian Government's efforts to improve cybersecurity. The ACSC provides advice and information about how to protect individuals and businesses online, and how to work with businesses, governments, academic partners and experts in Australia and overseas to investigate and develop solutions to cybersecurity threats.[105,106]

The Australian Prudential Regulation Authority (APRA) Prudential Standard CPS 234 on Information Security[107] applies to the banking, insurance and superannuation sectors, but provides a succinct overview of the objectives and key requirements for information security.

Examples of evidence

Examples of evidence may include:

Policy documents or contracts relating to the service provider's information security management system

Position descriptions that assign responsibilities for information security management actions

An audit and review schedule for information security

Reports from audits or reviews of information security management and action plans that remedy any identified issues

Analysis of incidents relating to information security management

Committee or meeting minutes that discuss or assess information security management of services

Records of conducting an information and data inventory

Feedback from the workforce on information security management.

Related actions

This action relates to Action 1.10 (risk management), Action 1.11 (incident management), Action 1.25 (safe environment), and Action 1.36 (continuity and updates).

Useful resources

1. ISO/IEC 27000 series. Available at: www.iso.org/standard/73906.html[104]
2. Cyber security. Available at: www.digitalhealth.gov.au/healthcare-providers/cyber-security[31]
3. Small Business Cyber Security Guide. Available at: www.cyber.gov.au/acsc/view-all-content/publications/small-business-cyber-security-guide[106]
4. Prudential Standard CPS 234 – Information Security. Available at: www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf[107]
5. Digital Health Security Awareness Course: Available at: https://training.digitalhealth.gov.au/enrol/index.php?id=14[108]
6. Australian Government Information Security Manual. Available at: www.cyber.gov.au/acsc/view-all-content/ism[109]

Continuity and updates

Action 1.36

The service provider:

a. Manages platform and operating system updates and patches
b. Manages the continuity of services, backup and recovery mechanisms
c. Effectively communicates service changes or interruptions to service users and, where relevant, their support people.

Intent of the action

Disruption to the digital mental health service from any cause is minimised through effective planning and communication.

Reflective questions

- How does the service provider manage updates and patches to services?
- What processes are in place to ensure that services can run effectively when there is a change or an interruption to the service?
- How does the service provider communicate with service users about any changes, interruptions, or discontinuation of the service?

Meeting the action

Ensuring the continuity of the essential functions of a digital mental health service in the event of a planned or unplanned change or interruption protects the interests of service users and the reputation of the service provider. Service providers must continually work to adapt to changes and risks that can affect their ability to provide continuity of service.

Managing change

A planned change to a digital mental health service may include a new software version, update or patch, or transition to a new digital platform or operating system. Patching for service modification or upgrade should be considered separately from patching for security issues, which should be linked closely to vulnerability management.

Unplanned disruptions may be caused by many factors, including hardware and software failures, cyberattack, data corruption, human error, weather events and natural disasters.

In all circumstances, it is important that there are systems in place to ensure continuity of the critical functions of the digital mental health service. This requires a risk assessment of the effect of an interruption on the functioning of the service, and a decision about what to do when a disruption occurs. This includes whether interim measures will be needed to cope with disruption.

Tasks for implementing the action:

- Engage service users, consumers, carers, families, and support people when designing the processes to be used to manage the continuity of digital mental health services
- Endorse a policy document and associated procedures about how to ensure continuity of the essential functions of a digital mental health service, including:
  - the agreed change management process
  - a contingency planning process
  - backup and recovery processes
  - a communication process
- Prepare documented risk management and impact assessments of the service provider's digital mental health services to guide the development of contingency plans for any disruption to service delivery
- Link continuity contingency planning with emergency and disaster management planning
- Train the workforce on managing planned updates and patches and unplanned interruptions of digital mental health services; focus on maintaining the safety of service users and ensuring continuity of the service.

Documentation of change management planning

Include in change management planning processes for:

- Identification and documentation of the requests for change
- Approval of the change, including listing checkpoints for rapid review before release of the proposed change
- Implementation and testing of the change
- Maintenance of system and security documentation, including a register of versions and histories of applications, patches, drivers, operating systems and firmware.

Business continuity and contingency planning

Tasks for implementing the action:

- Conduct an impact analysis to help identify and set priorities for information systems and components critical to supporting the continuity of the service provider's digital mental health services
- Identify preventive controls; these are measures that can be taken to increase system availability and reduce the effects of system disruptions
- Develop strategies to ensure the system can be recovered quickly and effectively following a disruption; include data backup and restoration processes that specify:
  - the location of data (such as alternative file servers)
  - the nature, frequency, and location of backup storage
  - the retention period
- Undertake plan testing, training, and exercises to validate recovery capabilities, prepare recovery personnel for plan activation, identify planning gaps, and improve overall organisational preparedness
- Maintain the plan and update it regularly to remain current with system enhancements and organisational changes.

Communication

Communication is an integral part of change management and the management of service disruptions.

Develop a process to clearly communicate to service users about:

- The steps that will be taken when there is a planned service change or unplanned interruption
- The level of essential functioning that will be maintained
- The extent of the planned change
- The level of risk associated with it.

Choose communication methods that will ensure service users will be fully informed before any change takes place.

To minimise any adverse impacts of changes, ensure that communication occurs well in advance of any planned interruptions of service.

Develop a crisis communications plan for unplanned disruptions. It should document standard procedures for internal and external communications, and assign roles and responsibilities.

Monitor and review the delivery of change

Tasks for implementing the action:

- Audit planned service iterations for compliance with the documented process, including compliance with checkpoints for rapid review before release of the next iteration, and take action to remedy any issues identified
- Periodically conduct desktop or simulated exercises that test the backup and recovery mechanisms to be used when an unplanned interruption occurs
- Regularly review service user complaints and incidents that relate to planned service, platform or operating system updates or patches, or unplanned interruptions.

Examples of evidence

Examples of evidence may include:

Policy documents about backup and recovery processes and about managing updates and patches to the platform and operating systems
Committee and meeting records that show planning for backup and recovery and managing updates and patches
Periodic review of backup and recovery systems
Communication to service users advising of service changes, interruptions or discontinuation of services
Analysis of incidents relating to changes to platform or operating systems, and action plans addressing any issues identified
Results of service user surveys on the communication provided about changes or interruptions to the service.

Related actions

This action relates to Action 1.10 (emergency and disaster management) and Action 1.35 (security and stability).

Useful resources

1. Fact sheet on applying the NSQDMH Standards using a risk management approach. Available at: www.safetyandquality.gov.au/publications-and-resources/resource-library/applying-nsqdmh-standards-using-risk-management-approach-fact-sheet[110]
2. ThinkUKnow: Preventing online child sexual exploitation. Available at www.thinkuknow.org.au[71]
3. National Principles for Child Safe Organisations. Available at: https://childsafe.humanrights.gov.au/national-principles[70]
4. ISO 13131:2021 Health informatics — Telehealth services — Quality planning guidelines. Available at: www.iso.org/standard/75962.html[111]
5. Professional Practice Guideline 19: Telehealth in psychiatry. Available at: www.ranzcp.org/files/resources/practice-resources/ranzcp-professional-practice-standards-and-guides.aspx[112]
6. Guidelines for technology-based consultations. Available at: www.medicalboard.gov.au/Codes-Guidelines-Policies/Technology-based-consultation-guidelines.aspx[113]
7. Telehealth guidance for practitioners. Available at: www.ahpra.gov.au/News/COVID-19/Workforce-resources/Telehealth-guidance-for-practitioners.aspx[114]
8. Australian Cyber Security Centre. Getting your business back up and running[115]
9. Guidelines for System Hardening. Available at: www.cyber.gov.au/acsc/view-all-content/advice/guidelines-system-hardening[116]
10. Vulnerabilities, exploits and threats. Available at: www.rapid7.com/fundamentals/vulnerabilities-exploits-threats[117]

Partnering with Consumers Standard

Service providers develop, implement, and maintain systems to partner with service users and their support people. These partnerships relate to the planning, design, delivery, measurement, review, and evaluation of digital mental health services. The workforce uses these systems to partner with service users and their support people.

Intention of this standard

To create services in which there are mutually valuable outcomes by having:

- Service users and their support people as partners in planning, design, delivery, measurement, review, and evaluation of digital mental health services
- Service users as partners in their own care, and with their support people, in line with the model of care and to the extent that they choose.

Criteria

Partnering with service users in their own care

Digital and health literacy

Partnering with service users in design and governance

Explanatory notes

Partnerships with consumers, carers, families and support people are integral to the development, implementation and evaluation of health policies, programs, and services. Service providers should ensure that these partnerships underpin the delivery of their digital mental health services.

Partnerships are effective when people are treated with dignity and respect, information is shared with them, and participation and collaboration in healthcare processes are encouraged and supported to the extent that people choose.

Delivering care that is based on partnerships provides many benefits for service users and their support people, and service providers. Effective partnerships are linked to positive experiences for service users, high-quality health care and improved safety.

Achieving effective partnerships when health care is delivered by digital means can occur at three levels, although the processes involved will vary according to the type of digital mental health service and its model of care.

At the **individual level**, partnership with the service user is shown by the delivery of respectful care and the provision of information relevant to the individual's care. Service users and, when appropriate, their support people, should be encouraged and assisted to take part in their own care and self-management, and engaged in making decisions and planning care, to the extent that they choose. This form of partnership is part of the way the service engages with the service user.

At the **level of a digital mental health service**, partnerships relate to the participation of service users, consumers, carers, families and support people in the planning, design, monitoring and evaluation of the digital mental health service and any changes in the service. Engaging with service users and their support people in the design of digital mental health services is essential to maximise the usability and accessibility of the service.

At the **level of the service provider**, partnerships relate to the involvement of service users, consumers, carers, families, and support people in overall governance, policy, and planning. This level overlaps with the previous level in that a service provider organisation may be made up of various digital mental health services. Service users, consumers, carers, families, and support people may be members of key committees for the service provider, in areas such as clinical governance, technical governance, service design, education, ethics and research.

Organisational leadership and support are essential to nurture partnerships at all three levels. Supporting effective partnerships with service users, consumers, carers, families, and support people may mean supporting several mechanisms for engagement.

Meaningful methods of engagement include representation on committees and boards, contributions to focus groups and providing feedback. They may occur face-to-face or via digital means. Taking the diversity of service users and their support people into account is necessary to achieve the best results. Developing meaningful partnerships may therefore take time and be an iterative process.

Strong leadership from governing bodies and executives can lay a solid foundation for adopting partnerships at all levels. It includes providing resources to support partnering activities (including training), and remuneration or reimbursement to help service users, consumers, carers, families and support people to actively participate.

To ensure that partnerships are meaningful and not tokenistic, service users, consumers, carers, families, and support people must be seen and treated as people with expert skills and knowledge. Monitoring, measuring, and evaluating consumer partnerships can help to ensure that the partnerships meet the needs of the service users as well as the service provider.

Usability

Usability is about how user-friendly a service is, including its ease of use, utility, and efficiency. It includes whether the service user can accomplish their goals effectively, efficiently, and satisfactorily by using the service.

When a digital mental health service is usable, service users quickly become familiar with it, find it easy to use during their first contact, and can readily recall how to use it on later visits.[118]

Accessibility

There are many barriers that can impede access to digital health services, including having a disability (including visual, auditory, physical, speech, cognitive, language, learning and neurological disabilities), speaking a language other than English, cultural factors, living in a location where telecommunication or internet services are limited and not having the capability or skills to operate the digital service. Factors relating to the digital hardware, software, platform and data requirements can also present barriers that impede use.

Around 1 in 5 Australians has a disability[119] and may face barriers when accessing digital mental health services. The *Disability Discrimination Act 1992* makes disability discrimination unlawful and promotes equal rights, equal opportunity, and equal access for people with disabilities.[120] A common disability in Australia is deafness. In 2014–15, 1 in 10 Australians was affected by total or partial deafness, with the proportion expected to increase as the population ages.[121,122]

Access to digital mental health services may be affected by age – for example, only 43% of Victorian adults aged 75 and older reported having internet at home in a 2017 survey, compared with over 90% of those aged between 18 and 54.[123] Although 91% of Australians have a smart phone, those aged 55 and over have been the slowest to embrace this technology.[124]

About 29% of the Australian population, or 7 million people, live in rural and remote areas and face challenges as a result of their geographic isolation, including having poorer health and welfare outcomes than people living in major cities.[125] Digital mental health services can offer access to health services that may not otherwise be readily available to them.

In 2019, 30% of Australians were born overseas.[126] In the 2016 Census, 4.9 million people reported speaking a language other than English at home, with over 300 separately identified languages spoken. The number of people who reported they spoke English 'not well' or 'not at all' was 820,000 (or 3.5% of the population).[126] Digital mental health services can assist in meeting the needs of service users who speak a language other than English by offering services in more than one language, linking with interpreter services, and ensuring they use jargon-free, plain English.

Criterion: Partnering with service users in their own care

Systems that are based on partnering with service users in their own care, and with their support people, are used to facilitate the delivery of care. Service users are partners in care, and with their support people, in line with the model of care and to the extent that they choose.

Person-centred care is the gold standard in healthcare delivery. Partnering with service users in their own care is an important pillar of person-centred care. It focuses on the relationship developed with the consumer and recognises that trust, respect and sharing of information are needed for the best health outcomes.

Given the variety of digital mental health services, partnering with service users may comprise many different and interwoven practices – from communication, structured listening and shared decision-making, to self-management support and care planning.

Key strategies to support service users to become partners in their own care may include:

- Providing health information in engaging and accessible formats
- Eliciting and documenting individual needs, preferences, and goals
- Using decision aids
- Encouraging and prompting service users to ask questions of the service
- Providing education to support self-management
- Providing information on self-help and support groups
- Developing tools and resources to encourage treatment adherence
- Providing service users with open access to their own healthcare record.

With the consent of the service user, service providers can also look at strategies for engaging with service users' support people, including carers and families, who can often provide unique insight into a service user's health history and provide valuable support and reassurance to the service user during their treatment.

Healthcare rights and informed consent

Action 2.01

The service provider uses a charter of rights that is:

a. Consistent with the Australian Charter of Healthcare Rights
b. Easily accessible to service users and their support people.

Intent of the action

Service users are aware of their healthcare rights and their rights are respected by service providers.

Reflective questions

- Does the service provider have a charter of rights that is consistent with the Australian Charter of Healthcare Rights?
- How are service users made aware of the service provider's charter?
- How do service users view and use the service provider's charter?

Meeting the action

The Australian Charter of Healthcare Rights[127] describes the rights that healthcare consumers, or someone they care for, can expect when receiving health care. These rights apply to all people in all places where health care is provided in Australia, including digital mental health services.

Review or develop a charter of rights

Service providers should adopt a charter of rights that is consistent with the Australian Charter of Healthcare Rights.

If the service provider does not have a charter of rights, use the Australian Charter of Healthcare Rights as a foundation for developing one. If necessary, adapt it to meet the specific needs of the service provider. However, the seven original rights must remain in place. If the service provider already has a charter of rights in place, review how it aligns with the Australian Charter of Healthcare Rights (2nd ed.).

Adopt the charter of rights

Tasks for implementing the action:

- Allocate responsibility for implementing and reviewing the charter to a designated position to support the effective adoption of the charter for digital mental health services
- Provide ready access to copies of the charter, in appropriate languages and formats, to all service users and, when relevant, their support people. Strategies may include:
  - incorporating information about the charter into communication with service users – for example, by adding it to the service provider's website
  - displaying information about the charter at the point of engagement with the digital mental health service
  - discussing the charter with service users, if possible
  - providing copies of the charter in a variety of languages reflecting service user populations
  - providing information in a format that is suitable for service users who are visually impaired, such as audio or on fully accessible websites
- Build the charter into organisational processes, policies, and codes of conduct, and outline how the rights in the charter will be achieved
- Provide orientation and education and training sessions for the workforce on their responsibilities for implementing the charter; include clinical and non-clinical members of the workforce and, if relevant, volunteers.

Review the effectiveness of the charter

Measure the impact of the charter to see whether promotion efforts are successful and whether this affects service user experience.

Strategies may include:

- Conducting surveys of service users to check whether they have been informed about the charter and understand what it means for them, and whether the rights in the charter have been respected
- Conducting surveys of the workforce about their awareness of, and attitudes towards, the charter
- Monitoring the engagement of service users and their support people with the charter (e.g. downloads of the charter).

Examples of evidence

Examples of evidence may include:

Policy documents that describe the use of a charter of rights
A charter of rights that is consistent with the Australian Charter of Healthcare Rights and available in different languages and formats, consistent with the service user profile
Observations showing that a charter of rights is accessible to service users
Information or resources that explain service users' healthcare rights
Evidence that service users received information about their healthcare rights and responsibilities – for example, audits of service users, interviews and surveys
A service intake checklist that includes provision and explanation of a charter of rights
Feedback from service users about their awareness of the charter of rights.

Useful resources

1. Australian Charter of Healthcare Rights (2nd ed.). Available at: www.safetyandquality.gov.au/consumers/working-your-healthcare-provider/australian-charter-healthcare-rights[127]
2. Supportive resources for the Australian Charter of Healthcare Rights (2nd ed.). Available from: www.safetyandquality.gov.au/consumers/working-your-healthcare-provider/australian-charter-healthcare-rights/supportive-resources-second-edition-australian-charter-healthcare-rights[128]
3. Charter on the Rights of Children and Young People in Healthcare Services in Australia. Available from: https://children.wcha.asn.au/publications/charter-rights-children-and-young-people-healthcare-services-australia[129]

Action 2.02

The service provider has informed consent processes that comply with legislation and best practice.

Intent of the action

Service providers ensure appropriate informed consent is explained and obtained whenever it is relevant to their processes and services.

Reflective questions

- How does the service provider ensure that the informed consent policy complies with legal requirements and best practice in informing consumers about the nature, risks and benefits of their services and what outcomes users can expect from using the services?
- How does the service provider monitor legal and policy compliance of its consent processes?

Meeting the action

Informed consent is a person's voluntary decision about their health care that is made with knowledge and understanding of the benefits and risks involved.[50] Consent may be explicit or implied.

Explicit consent is when a consumer clearly states their agreement to health care – for example, an examination or treatment. Implied consent occurs when the consumer indicates their agreement through their actions or by complying with a health practitioner's instructions. In the case of health care without substantial risk to the patient, it is usually sufficient to rely on a demonstration of the consumer's implied consent.[130]

Consideration should be given to seeking renewed consent when there has been a significant change to the condition or circumstances of the service user or to the nature of the direct care intervention being offered.

It is important that the information provided is clear and easy to understand if informed consent is to be achieved. This includes consideration of the format and language in which the information is provided and the mechanism by which informed consent is sought.

Research has found that consumers often do not read standard user terms and conditions.[66] This means seeking consent to health care via terms and conditions may not always be appropriate. Consent processes centred on acceptance of standard terms and conditions may also not recognise that consent may get outdated and no longer reflect a service user's preferences.[131]

Depending on the nature of the services being provided, a service provider may wish to implement a process whereby consent is specific to the actual healthcare component of the services and must be renewed after specified expiry dates. Such consent may better reflect user preferences and needs over time.

Consent policy

Tasks for implementing the action:

- Develop a comprehensive policy and procedures on informed consent by service users of digital mental health services, including:
  - when consent is implied – for example, when using information-only services
  - when consent is required – for example, when obtaining clinical treatment or providing sensitive personal information
  - how to assess the capacity of the service user
  - how consent is obtained
  - the need to be very clear about exactly what is being consented to
  - how consent will be documented – for example, in writing or by agreement to terms and conditions (informed by the nature, complexity, and level of risk of the digital mental health service)
  - when renewed consent is required
- Ensure that the informed consent policy takes into account the legislative requirements relating to the consent of minors and individuals who require support or substitute consent processes in the jurisdictions in which the digital mental health service will operate
- Link informed consent to the service provider's open disclosure policy
- Inform service users and, when relevant, their support people about the limitations, risks and benefits of the digital mental health service, including any fees and charges associated with it
- Schedule periodic reviews of the effectiveness and outcomes of the policy.

Support informed consent

Tasks for implementing the action:

- Provide information to service users in a way that they can understand before asking for their consent – for example, provide an accredited interpreter to help with communication, or adapt information into accessible formats (for example, by translating it into easy English or community languages, or providing it in audio or visual formats)
- Provide education and training to the workforce to support informed consent for digital mental health service interventions; including training on:
  - informed consent policy and procedures
  - effective communication to underpin good practice
  - legal, ethical, and practical foundations for service user consent
  - understanding of how individual health and digital literacy levels can act as barriers to understanding during the consent process
- Document service user consent to treatment (when applicable)
- Develop protocols for receiving, investigating and managing complaints about consent processes
- Seek feedback from service users about the processes for informed consent, and take action to deal with any issues identified.

Examples of evidence

Examples of evidence may include:

Policy documents for informed consent that reference relevant legislation or best practice and consider issues such as:

- when consent should be obtained
- when consent is not required
- how to get consent from service users from culturally and linguistically diverse backgrounds
- consent for young people
- training documents on informed consent processes

A standardised consent form that is in use

Results of audits of compliance with informed consent policies, procedures and protocols

Results of service user experience surveys, and actions taken to deal with issues identified about informed consent

Information packages or resources about treatment and consent processes; they should be available for service users in different formats and languages, consistent with the service user profile

Feedback about the consent process from service users.

Related actions

This action relates to Action 1.25 (terms and conditions), Action 1.32 (informed consent for data processes), and Action 2.03 (supported and substitute decision-making).

Useful resources

1. Guide to Informed Decision-making in Health Care: Available at: www.health.qld.gov.au/__data/assets/pdf_file/0019/143074/ic-guide.pdf[130]
2. Consent to Treatment Policy 2016. Available at: ww2.health.wa.gov.au/~/media/Files/Corporate/Policy-Frameworks/Clinical-Governance-Safety-and-Quality/Policy/WA-Health-Consent-to-Treatment-Policy/OD657-WA-Health-Consent-to-Treatment-Policy.pdf[132]

Action 2.03

The service provider has processes for supported decision-making, and to identify and work with a substitute decision-maker if a service user does not have the capacity to make decisions for themselves.

Intent of the action

Service users are supported to make decisions about their care wherever possible, and substitute decision-makers are involved in decision-making, if supported decision-making is not possible.

Reflective questions

- What decisions are service users asked to make in using digital mental health services?
- What processes are in place to identify a service user's capacity to make decisions about their own care?

Meeting the action

Develop a policy

Service users may be asked to make decisions about consent to care, data use and financial costs.

Under Australian law, all adults are presumed to have the capacity to decide whether they wish to receive health care, except when it can be shown that they lack the capacity to do so.

Tasks for implementing the action:

- Develop a policy that recognises service users' rights to make their own decisions including, if needed, getting support to make their own decisions, and outline the expectations for supported decision-making and when a substitute decision-maker may need to be involved
- Include information about supported decision-making and substitute decision-makers in service user communications about informed consent
- Periodically review the substitute and supported decision-making policy and procedures and evaluate whether they meet the needs of service users and reflect best practice.

Assessing capacity

Tasks for implementing the action:

- Work with service users, their support people and the digital mental health service workforce to develop procedures to support the policy, including guidance on:
  - assessing capacity in the context of the service provider's digital mental health services
  - identifying service users who require support in decision-making or for whom a substitute decision-maker may be required
  - assessing fluctuations in decision-making capacity
  - establishing considerations for special populations, such as children
  - incorporating cultural awareness
  - determining requirements for recording and documenting decisions
- Educate the workforce about assessing a service user's capacity to make decisions about their care, and about supported decision-making and substitute decision-making provisions

- Develop or provide resources and tools to reinforce training and assist the workforce to assess a service user's capacity to make decisions.

Processes to support decision-making

Decision-making support does not focus on whether a person can or cannot make decisions. It focuses on ensuring people have access to the right support they need to make, communicate and take part in decisions.

Assistance may take many forms including getting an interpreter, using plain language and simple sentences when communicating, using pictures, or giving the person more time in which to make a decision. Support is aimed at acknowledging, interpreting and acting upon a person's will and preference. This process focuses less on the who of the decision-making process, and more on the how as well as the why service users want to make a particular decision.[133]

Tasks for implementing the action:

- Educate the workforce about supported decision-making provisions
- Ensure all members of the workforce adopt a collaborative approach that allows support people to be involved in decision-making
- Reframe treatment decisions in the wider context of the service user's wishes, values and goals, and of what they consider of relevance in their life
- Implement safeguards to ensure that the potential for influencing decisions or abuse of power is recognised and minimised.

Processes to identify substitute decision-makers

If a service user does not have the capacity to make decisions about their own care, even with support, a substitute decision-maker may be required.[130]

Service providers should consider how substitute decision-makers may be involved in consent for digital mental health services, and incorporate a list of appropriate substitute decision-makers into the organisation's informed consent policy.

Advance care directives

An advance care directive is an instruction that a person makes about their future medical treatment or health care, in the event he or she loses capacity to make decisions. They can record directions about care and treatments and, in some jurisdictions, can formally appoint a substitute decision-maker. To meet this requirement:

- Include advice in the informed consent policy on how an advance care directive may apply when a digital mental health service user has impaired decision-making capacity
- Establish a process that determines whether an advance care directive is in place for a service user.

Examples of evidence

Examples of evidence may include:

Policy documents or processes for:

- identifying a patient's capacity for making decisions about their care
- identifying a substitute decision-maker, if a patient does not have the capacity to make decisions about their care
- documenting the persons responsible for making substitute decisions – for example, legal (including enduring) guardians, spouses, carers, close friends or relatives, or an appropriate tribunal

Results of audits of healthcare records that identify patients' capacity to make decisions and confirm the identity of the substitute decision-maker, if required

Results of audits of healthcare records for compliance with policies, procedures and protocols, and completeness of documentation relating to advocacy or guardianship.

Useful resources

1. Capacity Australia. Available at: https://capacityaustralia.org.au[134]
2. Advance Care Planning Australia. Available at: www.advancecareplanning.org.au[135]
3. Impaired Decision-Making Factsheet. Available at: www.sahealth.sa.gov.au/wps/wcm/connect/public+content/sa+health+internet/resources/what+is+impaired+decision+making+capacity+and+how+is+it+assessed+factsheet[136]
4. United Nations Convention on the Rights of Persons with Disabilities. Available at: www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities.html[137]
5. Scottish Health Council's Participation Toolkit. Available at: www.hisengage.scot/toolkit.aspx[138]
6. Gillick Competency Principles: Can children and adolescents consent to their own medical treatment? Available at www.racgp.org.au/afpbackissues/2005/200501/200501bird.pdf[139]
7. Application of legal and ethical issues to young people. Available at: www.health.nsw.gov.au/kidsfamilies/youth/Documents/youth-health-resource-kit/youth-health-resource-kit-sect-3-chap-5.pdf[140]
8. Guidelines for Supported Decision-Making in Mental Health Services. Available at: https://healthtalkaustralia.org/wp-content/uploads/2019/04/Guidelines-for-Supported-Decision-Making-in-Mental-Health-Services.pdf[141]

Planning care

Action 2.04

The service provider has processes to partner with service users and, where relevant, their support people to make decisions about their current and future care.

Intent of the action

Service users receive safe and high-quality care by being involved in decisions and planning about current and future care.

Reflective questions

- How does the service provider partner with service users to plan, communicate, set goals, and make decisions about current and future care?
- How does the service provider review its processes for partnering with service users?

Meeting the action

Partnering with service users in their own care is integral to the delivery of safe and high-quality person-centred health care and should remain a clear focus for digital mental health services.

Create a person-centred care culture

The service provider should set clear expectations that its digital mental health services will provide person-centred care.

Tasks for implementing the action:

- Promote the importance of partnerships with service users and show this commitment by incorporating it into the strategic planning, vision, and goals
- Engage service users, consumers, carers, families, and support people in governance and strategic planning to support digital mental health service provision
- Set specifications for the design of digital mental health services around partnering with service users, including self-management options, interactive features and capacity to ask questions and provide feedback.

Enable partnering with service users in their own care

Service users can be partners in their own care in many ways, including shared decision-making, self-management, and personalised care planning. Strategies for involving service users in care planning may include systematically discussing their preferences at the time of their engagement with the digital mental health service, and at regular times during their care. Good communication underpins a partnership approach and is vital to foster trust and respect.[142]

Tasks for implementing the action:

- Endorse a policy and associated processes to involve service users and, when relevant, their support people or substitute decision-maker, in planning, communication, goal-setting and decision-making for the service user's current and future care
- Work with service users, their support people and the digital mental health service workforce to develop procedures to support the policy, including guidance on partnering with service users in their own care when using digital mental health services
- Promote self-management options, when appropriate, to enhance service

user engagement and encourage them to ask questions

- Provide service users with ready and open access to their healthcare data and records
- Engage with service users and, when relevant, their support people, to check the information that is provided to them by digital mental health services, and how it is provided, and identify any communication barriers and areas for improvement to ensure that it meets their needs
- Implement an education and training program to develop the skills of the health workforce to partner with digital mental health service users in their care.

Measure and monitor partnering with service users

It is important to measure and monitor the quality of partnering with service users in digital mental health services. This can be done by:

- Collecting formal feedback from service users and, when relevant, their support people using measurement tools, focus groups and surveys
- Asking service users to self-report on their experience and satisfaction with the level of engagement they had in their care.

If specific input from service users is not available – for example, when service users are anonymous – engage with consumers, carers and families more broadly to inform improvement approaches.

Examples of evidence

Examples of evidence may include:

Policy documents about partnering with service users in their care, including policies on communication and interpersonal skills, shared decision-making and health literacy

Training documents about partnering with service users in their care and in shared decision-making

Results of audits of healthcare records to identify the involvement of clinicians and service users in developing a plan of care

Analysis of feedback data from the workforce about partnering with service users in their care.

Related actions

This action relates to Action 1.13 (feedback) and Action 1.31 (transparency).

Useful resources

Partnerships at the individual and service provider level

1. Partnering with patients, carers and families. Available at: www.cec.health.nsw.gov.au/improve-quality/teamwork-culture-pcc/partnering-with-people/partnering-with-patients[143]
2. Patient-Centered Care Improvement Guide. Available at: https://resources.planetree.org/patient-centered-care-improvement-guide[144]
3. Patient and Family-Centred Care Toolkit. Available at: www.pointofcarefoundation.org.uk/resource/patient-family-centred-care-toolkit[145]
4. Working with Women Engaged in Alcohol and Other Drug Treatment (2nd ed.). Available at: https://nada.org.au/wp-content/uploads/2021/01/working_with_women_engaged_in_aod_treatment_web.pdf[146]

Shared decision-making

1. The SHARE Approach: A Model for Shared Decision Making. Available at: www.ahrq.gov/sites/default/files/publications/files/share-approach_factsheet.pdf[147]
2. Shared decision making. Available at: https://www.nice.org.uk/about/what-we-do/our-programmes/nice-guidance/nice-guidelines/shared-decision-making[148]
3. MAGIC: Shared decision making. Available at: www.health.org.uk/funding-and-partnerships/programme/magic-shared-decision-making[149]

Criterion: Digital and health literacy

The service provider takes account of the health and digital literacy of service users and ensures that communication occurs in a way that supports effective partnerships.

Health literacy refers to how people understand information about health and health care, and how they apply that information to their lives, use it to make decisions and act on it. **Digital literacy** refers to the ability to identify and use technology confidently, creatively, and critically to meet the demands and challenges of life, learning and work in a digital society.

While health literacy plays an important role in facilitating communication and enabling effective partnerships with service users, digital literacy is important to enable the most effective use of digital mental health services.

The Commission separates health literacy into two components.[150]

Individual health literacy is the skills, knowledge, motivation, and capacity of a person to gain access to, understand, appraise, and apply information to make effective decisions about health and health care, and take appropriate action.

Health literacy environment is the infrastructure, policies, processes, materials, people, and relationships that make up the healthcare system and affect the way that people gain access to, understand, appraise and apply health-related information and services.

The Health Literacy Survey conducted in 2018 noted that 8% of Australians find it difficult to understand health information well enough to know what to do. Although almost 90% found it easy to discuss health concerns and actively engage with healthcare providers, only 17% of people who reported very high levels of psychological distress found it always easy to navigate the healthcare system.[125]

Digital health literacy occurs at the intersections of literacy, digital literacy, and health literacy and is the ability to find, understand, and evaluate health information from electronic sources, and apply the knowledge gained to prevent or solve a health problem.[151]

To achieve digital health literacy, individuals must be able to navigate the many digital technologies available (e.g. internet, apps), locate relevant digital mental health services, navigate each site (e.g. open and close browsers or apps, navigate pages and tabs), interpret graphics and images, interpret and synthesise the health information provided (which may be conflicting if many sources are perused), understand the meaning of any specialised vocabulary used, check the credibility of sources, enter data and communicate digitally with a provider.[152,153]

The digital health literacy of consumers may be affected by age, education, disability, culture, language, and geography. Service providers have a responsibility to build a digital health literacy environment that supports effective partnerships with service users. This includes reducing unnecessary complexity for service users when using and navigating the digital mental health service.

Digital universal precautions are best practices, instituted in a standardised fashion, to improve communication and participation for all service users regardless of health literacy.[154] Communication can be improved by using a co-design approach that engages with consumers and carers about content, readability, formatting and accessibility.

Communication that supports effective partnerships

Action 2.05

The service provider uses communication mechanisms tailored to the diversity of service users and their support people.

Intent of the action

Service users receive the information they need in a way that is appropriate for them.

Reflective questions

- How are the communication needs of diverse service users identified?
- What strategies are used to tailor communication to meet the needs of diverse service user populations?

Meeting the action

There is no 'one size fits all' solution to meeting the communication requirements of a diverse service user population. Diversity comes in many forms – for example:

- Language factors may affect service users for whom English is not their first language, as well as those with low literacy skills, cognitive impairment or a physical condition such as deafness or blindness
- Cultural factors may affect service users from culturally and linguistically diverse communities and Aboriginal or Torres Strait Islander peoples
- Digital literacy may affect the ability to find, navigate, or use a service
- Location may influence the digital options available for communication.

Emphasise diversity of communication

Tasks for implementing the action:

- Administer surveys to collect demographic information and understand the diversity and communication needs of service users
- Engage consumers, carers, and families in the design of digital mental health services to maximise the effectiveness of the communication tools used by the services.

Enable diverse communication

Tasks for implementing the action:

- Implement communication mechanisms that meet the needs of specific populations – for example, by providing the digital mental health service in different languages or in various culturally appropriate formats
- Provide cultural safety training if Aboriginal and Torres Strait Islander communities regularly use the digital mental health services or are part of the intended user group
- Educate the workforce about the diversity of service users
- Make accredited interpreter services available for service users who require them; periodically review their usage
- Endorse a framework, such as universal digital precautions, to assist digital mental health services to meet the communication needs of a diverse service user population.[154]

Monitor and measure diversity of communication

Tasks for implementing the action:

- Periodically seek feedback from service users and, when relevant, their support people on the effectiveness of the communication tools used in meeting their needs; take action to remedy any issues identified
- Assess the cultural competency and confidence of the workforce in communicating with diverse service user populations and seek feedback from diverse service user populations about whether they find the service culturally safe.

Examples of evidence

Examples of evidence may include:

Policy documents about communication and addressing the diversity of the communities that the service provider serves

A demographic profile or demographic survey for the service provider that identifies the diversity of its service users

Results of an assessment of the communication needs of service users

Demographic data from external sources that are used as part of strategic and communication planning to help identify the diversity and needs of service users

Training documents about cultural awareness and diversity

Service user information or resources that are culturally appropriate, and are available in various languages and accessible formats

Feedback from service users from diverse backgrounds during the development or review of information packages or resources

Committee and meeting records that show that the service provider is responding to the needs of the service user population

Reports on use of interpreters

Feedback from service users and carers about whether communication processes meet their needs

Observations that clinicians have access to communication resources that provide contact details for support services such as local service user health advocates, interpreters and cultural support and liaison services.

Useful resources

1. National Statement on Health Literacy. Available at: www.safetyandquality.gov.au/publications-and-resources/resource-library/national-statement-health-literacy-taking-action-improve-safety-and-quality[150]
2. NSW Health Literacy Framework. Available at: www.cec.health.nsw.gov.au/__data/assets/pdf_file/0008/487169/NSW-Health-Literacy-Framework-2019-2024.pdf[155]
3. Health Literacy Framework: A Guide to Action. Available at: www.cec.health.nsw.gov.au/improve-quality/teamwork-culture-pcc/person-centred-care/health-literacy[156]
4. Health Translations Directory (links to reliable translated health resources produced in Australia). Available at: https://healthtranslations.vic.gov.au[157]
5. Agency for Healthcare Research and Quality Health Literacy Universal Precautions Toolkit (2nd ed.). Available at: www.ahrq.gov/sites/default/files/publications/files/healthlittoolkit2_3.pdf[158]
6. Health Literacy. Available at: www.cdc.gov/healthliteracy[159]
7. Simply Put: A guide for creating easy-to-understand materials. Available at: www.cdc.gov/healthliteracy/pdf/simply_put.pdf[160]
8. Health Literacy: Find Training. Available at: www.cdc.gov/healthliteracy/gettraining.html[161]
9. The Plain Language Action and Information Network. Available at: www.plainlanguage.gov[162]
10. Health Literacy resources. Available at: https://health.gov/our-work/national-health-initiatives/health-literacy[163]
11. Digital Universal Precautions. Available at: https://pubmed.ncbi.nlm.nih.gov/31171391[154]
12. Centre for Culture, Ethnicity and Health. Supportive systems for health literacy. [Internet] [cited 2022 Jan 31]. Available at: www.ceh.org.au/resource-hub/supportive-systems-for-health-literacy[164]
13. Health Consumers Queensland – Consumer Representatives Program: Agency handbook. Available at: www.health.qld.gov.au/__data/assets/pdf_file/0028/425944/agen_handbook.pdf[165]
14. Can They Understand? Testing Patient Education Materials With Intended Readers. Available at: https://healthliteracy.com/2001/11/01/testing-materials-with-readers[166]
15. DISCERN Instrument. Available at: www.discern.org.uk/discern_instrument.php[167]

Action 2.06

The service provider communicates information to service users and, where relevant, their support people:

a. In a way that meets their needs

b. That is easy to understand and use.

Intent of the action

Service users receive the information they need to get the best health outcomes, and this information is easy to understand and act on.

Reflective questions

- How does the service provider assess whether the communication of information to service users meets their needs and is easy to understand?

Meeting the action

Clear and open communication with service users and, when relevant, their support people can increase trust in digital mental health services, promote self-management, and promote partnerships and the delivery of effective, efficient, and ethical healthcare. This includes the management of any deterioration.[168]

Information for service users should be available as needed, suitable to the digital environment.

Service user information should be at a level that can be understood and used by diverse service users. Culture and language should be considered and reflect the diversity of the service user population. The use of interpreters may be an option in some digital mental health services, but the service provider should ensure that interpreters have the skills required for the role.

Support appropriate communication

Conduct an assessment to work out which methods may best suit the communication purposes of the digital mental health service. For example, an internet site may be useful for giving complex or lengthy information and links to external sources (and enables a service user to easily refer back to the information), whereas chatbots or text messaging may be preferable for quick queries. In addition:

- Implement a policy that outlines health and digital literacy requirements for digital mental health services
- Assign responsibility to an individual or group for actions to improve the health literacy environment of digital mental health services
- Engage with service users, consumers, carers, families and support people to develop information resources and tools to support communication
- Identify or develop a variety of information resources for service users, so that information that meets the needs of individual service users is available
- Ensure that the information provided to service users and their support people remains current
- Provide training and resources to the workforce about digital communication methods
- Provide the workforce with access to appropriate service user information resources and tools to support communications and ensure that any tools and resources remain current.

Monitor and measure appropriateness of communication

Tasks for implementing the action:

- Use analytics to study the use of digital information, tools and resources
- Review complaints and feedback from service users and, when relevant, their support people about information made available to them via digital mental health services, to assess whether the information provided met their needs
- Conduct an audit of the health literacy environment of the service provider's digital mental health services and take action to remedy any issues identified.

Examples of evidence

Examples of evidence may include:

Policy documents about communication, including the use of plain language, health literacy, and addressing the needs of service users

Results of a needs assessment project that identifies service user information needs

Training documents about communication methods

Service user information packages or resources that show ease of understanding and use

Feedback from service users during the development or review of information packages or resources, and the actions taken in response to the feedback

Feedback from service users about whether communication processes meet their needs.

Useful resources

1. Health literacy. Available at: www.safetyandquality.gov.au/our-work/patient-and-consumer-centred-care/health-literacy[169]
2. Guide for Engaging with Consumers and the Community, Tool 3 – Tips for communicating clearly. Available at: www.sahealth.sa.gov.au/wps/wcm/connect/6dead9da-d1c2-4cbf-9568-74d2131df162/EngagingwithConsumersCarersandCommunityGuide%26Resources_Apr+2021+%281%29.pdf[170]
3. Cue Cards in Community Languages. Available at: www.easternhealth.org.au/site/item/152-cue-cards-in-community-languages[171]
4. Health Literacy Online. Available at: https://health.gov/healthliteracyonline[172]

Criterion: Partnering with service users in design and governance

The service provider partners with service users and their support people in the design and governance of digital mental health services.

Involving consumers, carers, and families in health decision-making adds value by improving quality of care, efficiency of resource use, and community support for programs or services.[173] Partnering with consumers, carers and families is a key element in discussions and decisions about the design, implementation and evaluation of health policies, programs and services.[174,175]

Methods of partnership range from informal, one-off events or feedback through social media to formal participation in design processes and ongoing participation on boards and committees. Engagement may be as an individual, or in small or large groups, and should be guided by the nature of the digital mental health service, the role that is required, and the diversity of the service user population.[174]

In the planning and design of a digital mental health service, engaging consumers and carers from the intended user group for the service, along with health practitioners and other stakeholders, in the planning and design of a digital mental health service will improve understanding of both user and stakeholder needs. It can be part of an iterative process of design and service development. Service providers may choose to engage external expertise in a co-design process.

Partnerships in governance, planning, design, measurement and evaluation

Action 2.07

The service provider:

a. Partners with consumers, carers and families from the intended service user groups in the governance, planning, design, measurement and evaluation of the services

b. Has processes to involve a mix of people that are reflective of the diversity of service users and their support people.

Intent of the action

The diversity of service users and their support people helps shape the way the service provider operates its digital mental health services to achieve mutually beneficial outcomes.

Reflective questions

- How does the service provider involve service users, consumers and carers in the governance, planning, design, measurement and evaluation of services?
- What processes are in place to ensure that the diversity of service users is reflected in these partnerships?
- How does the service provider review and evaluate their processes for partnering with service users, consumers, carers, families and support people?

Meeting the action

Develop a framework

Supporting partnerships in governance and strategic leadership may involve service users and their support people, or members of the broader consumer and carer community.

Opportunities include involvement on boards, committees and advisory groups, participating in workforce recruitment and workforce training, and developing information about safety issues, such as potential risks of care. Shaping the attitudes of the workforce is important so that there is greater acknowledgement, acceptance and understanding of the value of consumer input.

Consumers and carers can provide unique insights into safety and quality issues and risks, including which issues should have priority, and which solutions are acceptable. Engaging service users, consumers, carers, families, and support people in measuring and evaluating the safety and quality of digital mental health services can occur in many ways, including involving them in planning and implementing safety and quality improvement activities and in evaluating feedback data. When doing so:

- Clearly articulate the desire of the governing body to support, promote, and improve partnerships with service users, consumers, carers, families and support people in governance, planning, design, measurement, and evaluation
- Engage organisational leaders to act as champions for these partnerships
- Develop a framework and systematic processes for partnering, with input from the wide variety of service users, consumers,

carers, families, support people, the workforce and other key stakeholders, and ensure that it is relevant to the type of digital mental health service, its stage of development, and the nature of the service user partnership being sought

- Co-design digital services with consumers, carers and families as well as other relevant stakeholders such as decision-makers, clinicians and peer workers, and continue their involvement during implementation and iterative adaptation of digital mental health services.

Implement a partnership approach

Tasks for implementing the action:

- Create a leadership position with responsibility for improving the service provider's commitment to service user partnership
- Review the current level of service user partnerships in governance, strategic and operational planning, digital mental health service design, and measurement and evaluation of safety and quality performance, and identify any barriers to effective partnerships
- Establish meaningful positions for service users, consumers, carers, families and support people on formal governance committees, and create advisory groups that provide direct input to leadership and management structures
- Educate the workforce to improve their understanding of the roles for consumer partners in governance and strategic leadership
- Provide multiple opportunities for service users to provide feedback on the safety and quality of services via feedback channels within the digital mental health service, surveys, or focus groups.

Hearing the many voices of service users is important. Include, when relevant, Aboriginal and Torres Strait Islander peoples, culturally and linguistically diverse groups, LGBTIQ+ people, people from lower socioeconomic groups and rural and remote locations, as well as youth and older people. This can also inform the cultural safety of the service provider's digital mental health services.

Varied strategies and engagement methods may be needed for different people, groups and communities. Strategies might include engaging with leaders or liaison officers of identified groups to discover the most appropriate engagement strategies for their community, or inviting representatives from these groups to join the governing body or be involved in consumer advisory groups.

Examples of evidence

Examples of evidence may include:

Policy documents that describe the service provider's requirement for partnering with service users, consumers, and carers, including in governance, planning, design, measurement and evaluation

Training documents for management and the workforce about partnering with service users in governance, planning, design, measurement and evaluation

Tools to support partnering with service users, consumers and carers

Minutes of committee meetings that show the participation of service users, consumers and carers in governance, planning, design, measurement and evaluation

Recruitment processes that engage service users, consumers and carers as partners in governance, planning, design, measurement and evaluation

Observations of service users, consumers and carers taking part in making decisions about governance, planning, design, measurement and evaluation.

Useful resources

1. Partnership Self-Assessment Tool. Available at: www.nccmt.ca/knowledge-repositories/search/10[176]
2. Health Care Providers' Guide to Engaging Multicultural Communities and Consumers. Available at: www.health.qld.gov.au/multicultural/support_tools/engage-guide[177]
3. How to co-design with young Victorians. Available at: www.vichealth.vic.gov.au/media-and-resources/publications/co-design[178]
4. Health service co-design toolkit. Available at: www.healthcodesign.org.nz[179]
5. A Guide to Build Co-design Capability. Available at: www.aci.health.nsw.gov.au/__data/assets/pdf_file/0013/502240/Guide-Build-Codesign-Capability.pdf[180]
6. Guide for Developing a Community-Based Patient Safety Advisory Council. Available at: www.ahrq.gov/research/findings/final-reports/advisorycouncil/index.html[181]
7. Getting Started toolkit. Available at: https://hic.org.au/toolkit-for-health-services[49]
8. Making Change: Designing Change Projects. Available at: https://aci.health.nsw.gov.au/resources/redesign/change/making-change/designing[182]
9. Experience-based co-design toolkit. Available at: www.pointofcarefoundation.org.uk/resource/experience-based-co-design-ebcd-toolkit[183]
10. Patient and Family-Centred Care toolkit. Available at: www.pointofcarefoundation.org.uk/resource/patient-family-centred-care-toolkit[145]
11. Guide for Engaging with Consumers and the Community. Available at: www.sahealth.sa.gov.au/wps/wcm/connect/6dead9da-d1c2-4cbf-9568-74d2131df162/EngagingwithConsumersCarersandCommunityGuide%26Resources_Apr+2021+%281%29.pdf[170]
12. The Participation Toolkit. Available at: www.hisengage.scot/toolkit.aspx[138]
13. Co-production: Putting principles into practice in mental health contexts. Available at: https://healthsciences.unimelb.edu.au/__data/assets/pdf_file/0007/3392215/Coproduction_putting-principles-into-practice.pdf[184]
14. Champions of Inclusion: A Guide to Creating LGBTIQ+ Inclusive Organisations. Available at: www.lgbtiqhealth.org.au/championing_inclusion[185]

Action 2.08

The service provider provides orientation, support and education to service users, consumers, carers, families and support people who are partners in the governance, planning, design, measurement and evaluation of the service.

Intent of the action

Service users partnering in organisational design and governance have the skills and knowledge they need to be able to contribute effectively and safely.

Reflective questions

- What training and support are offered to service users who are partnering in the governance, design, measurement and evaluation of the service provider?
- How is feedback from service users used to evaluate and improve the effectiveness of the support provided?

Meeting the action

Provide comprehensive training and support

Providing comprehensive training and support for service users, consumers, carers, families and support people involved in the organisation's governance processes, planning, design, measurement or evaluation activities gives them the best opportunity to contribute meaningfully and effectively to the service provider and its digital mental health services.

Service providers may not have the capacity to develop comprehensive training and resources. These providers should look to adapt resources from similar organisations, or arrange access to external training programs provided by consumer organisations and other groups.

Tasks for implementing the action:

- Endorse a remuneration policy for service users, consumers, carers, families and support people who are partners in governance, planning, design, measurement and evaluation activities to reflect the value and importance of their input
- Employ a facilitator or coordinator to engage with, support, and build the confidence of, current and potential partners
- Inform service users and their support people that the information they provide is separate from the process of providing or receiving care and will not affect their treatment
- Provide opportunities for service users, consumers, carers, families and support people who work with the service provider to comment or to raise concerns about the process if they wish.

Use consumer information respectfully

Information provided by service users, consumers, carers, families and support people about their experiences must be treated sensitively.

Tasks for implementing the action:

- Ensure that privacy and confidentiality is maintained for service users, consumers, carers, families and support people who partner with the service provider, and that they share their experiences and stories only to the extent that they are comfortable

- Act on the information provided by service users, consumers, carers, families and support people, if feasible, and inform them about changes that have occurred because of their input and advice.

Examples of evidence

Examples of evidence may include:

Orientation and training resources for service users, consumers, and carers to support their partnering in governance, planning, design, measurement and evaluation

Feedback from service users, consumers, and carers about their experiences of orientation, support, and education to help them take part in governance, planning, design, measurement and evaluation

Surveys of service users, consumers and carers about the support and education needed to aid their participation in governance, planning, design, measurement and evaluation

A position description for the role of a consumer engagement coordinator or facilitator.

Related actions

This action relates to Action 1.15 (diversity and high-risk groups), Action 2.10 (usability) and Action 2.11 (accessibility).

Useful resources

1. Consumer and Carer Engagement: a Practical Guide. Available at: www.mentalhealthcommission.gov.au/mental-health-reform/consumer-and-carer-engagement/consumer-and-carer-engagement-a-practical-guide[186]
2. A practical guide for working with carers of people with a mental illness. Available at: https://mhaustralia.org/publication/practical-guide-working-people-mental-illness[187]
3. Health Issues Centre accredited courses. Available at: https://hic.org.au/accredited-courses[188]
4. Guidelines for Consumer Representatives. Available at: https://chf.org.au/guidelines-consumer-representatives[189]
5. Cancer Australia Consumer Involvement Toolkit: Available at: https://consumerinvolvement.canceraustralia.gov.au[190]

Action 2.09

The service provider partners with service users and their support people to incorporate their views and experiences into training and education for the workforce.

Intent of the action

The workforce has an understanding of health care from the service user's perspective, and the value that consumers can bring to organisational design and governance.

Reflective questions

- How does the design and delivery of workforce training and education by the service provider reflect the involvement of service users?

Meeting the action

Whole-of-organisation training is essential to increase understanding of service user experiences, make explicit the connection between person-centred service delivery and service user recovery, and encourage genuine collaboration with service users and their support people. Training should be ongoing and revisited, rather than a one-off.

Tasks for implementing the action:

- Implement a policy that involves service users and their support people in the design and delivery of workforce training, and reimburses them appropriately
- Review current workforce training processes, materials and resources to identify how they can be modified to include service users and their support people
- Involve service users and their support people in an advisory capacity or in delivering training by:
  - convening focus groups or workshops to seek service users' advice on critical information, training materials, resources and strategies for training the workforce in person-centred care and partnerships
  - inviting service users and their support people to attend and review training sessions to ensure that the training reflects their needs and perspectives
  - inviting service users and their support people to present on their experiences at training sessions for the workforce, or use video or audio recordings of personal stories from consumers or carers
- Ensure that when service user accounts are used in training, their information is treated sensitively, that privacy and confidentiality are maintained, and that service users are supported to share their experiences and stories to an extent to which they are comfortable
- Consult regularly with service users and their support people to seek their views and input for the updated development and delivery of workforce training
- Review lessons learned from service user feedback and complaints and incorporate this into workforce training
- Survey the workforce on training provided in partnership with service users and their support people and identify opportunities to improve the training.

Examples of evidence

Examples of evidence may include:

Policy documents that describe the approach to training and educating the workforce, including the need to incorporate the views and experiences of service users

Training and education resources that show that the views and experiences of service users have been incorporated

Assessment of the training and education needs of the workforce, and responses to this that incorporate the views and experiences of service users

Recruitment of service users as trainers or educators

Analysis of service user feedback and complaints; give priority to issues to be incorporated into workforce training and education.

Useful resources

1. Patient-Centered Care Improvement Guide. Available at: https://resources.planetree.org/patient-centered-care-improvement-guide[144]
2. Consumer Involvement Toolkit. Available at: https://consumerinvolvement.canceraustralia.gov.au[190]
3. Storytelling for health services. Available at: https://consumerinvolvement.canceraustralia.gov.au/document-library/service-managers/storytelling-health-services[191]
4. Guidance for Collecting & Using People's Stories. Available at: www.healthwatchcambridgeshire.co.uk/sites/healthwatchcambridgeshire.co.uk/files/peoples_stories_guidance_0.pdf[192]
5. Collecting Patient and Carer Stories. Available at: https://aci.health.nsw.gov.au/resources/redesign/change/making-change/Guide_to_collect_patient_carer_stories.pdf[193]
6. Patient Stories: A toolkit for collecting and using patient stories for service improvement in WA Health. Available at: www.safetyandquality.gov.au/sites/default/files/migrated/A_toolkit_for_collecting_and_using_patient_stories.pdf[194]

Usability

Action 2.10

The service provider has processes to assess and optimise the usability of each service including:

a. Function
b. Cultural safety
c. Service user feedback, experience and satisfaction
d. Service user outcomes
e. Access.

Intent of the action

The functioning of the service is optimised for service users and the experience of using the service is positive for the service user.

Reflective questions

- How are service users involved in the development and review of the service to optimise functionality?
- How does the service provider engage with service users to assess the cultural safety of the service?
- How does the service provider optimise the use of the service by the intended users?
- What processes are in place for the service provider to assess the level of satisfaction of service users with the service?

Meeting the action

Usability is part of the broad term '**user experience**'. User experience is about how a service user interacts with, and experiences, a service. It includes their perceptions and reactions to the usability of the service, and incorporates features such as the interaction design and the visual design of the service – before, during and after use. User experience is subjective in nature and changes as usage circumstances change. It is more complex than just creating good usability. Even so, good usability can help build a relationship with the service user.[118]

Cultural safety can affect usability because it derives from how the care is provided, rather than what care is provided, and is defined not by the service provider but by the service user's experience. Embedding cultural safety means Aboriginal and Torres Strait Islander peoples will be more likely to get healthcare services and experience better outcomes when they do.[23]

User-centred design is based upon an explicit understanding of users, tasks, and environments and is driven and refined by user-centred evaluation. Engaging with service users is therefore key to optimising usability and user experience.

Prototypes may be used to test different service designs and solutions and measure the usability of a digital mental health service as work progresses. Usability testing should begin early in the design process and focus on testing the service's design features in the service user's context. Service providers should look at what the service user wants to do with the service, in their environment. They should look at how easy it is to find and use, whether the service design functions as it should, and if the user can do what they need to do in the service.

Tasks for implementing the action:

- Identify intended service users and work with them to understand their needs and what they are looking for in using the service
- Allocate enough resources to support best usability and user experience
- Engage with consumers and carers from the intended service user groups in the design and development of a new digital mental health service, and conduct usability testing during the design and development phase and regularly thereafter
- Use the outcomes of usability testing to iteratively improve the service design
- Engage in usability testing with a variety of participants, including service users with disabilities and other diverse population groups, to understand how these groups will experience the digital mental health service
- For existing digital mental health services, review the information architecture, content, language, workflow, and consistency to ensure that they meet user needs (including cultural safety) as well as the business objectives of the service
- Keep records of the results of usability testing and how the design of the service changed in response
- Provide options to support users while they are using the service – for example, a pop-up chat box or a telephone number to call for technical advice
- Provide information on the usability of the service through the product information developed for potential service users (see Action 3.03)
- Review feedback and complaints about the usability of the service, and take action to remedy any issues identified
- Identify and collect indicators that inform about usability and service user experience – for example, return rate and average time spent on a web page
- Undertake a self-assessment against a maturity matrix for usability of the service and take action to move to the next level.

Examples of evidence

Examples of evidence may include:

Committee and meeting records that show service user involvement in the development and review of services

Feedback from service users who have been engaged in the development and review of services

Evaluation reports about services that identify how service users were involved in development and review

Examples of services that have changed in response to service user feedback

Communication with service users who provided input into the development or review of services, including about the types of changes made in response to their participation and feedback.

Related actions

This action relates to Action 1.15 (diversity), Actions 1.25, 1.26 and 1.27 (safe environment), Actions 2.05 and 2.06 (communication), Action 2.07 (partnering), Action 2.11 (accessibility) and Action 3.02 (model of care).

Useful resources

1. Maturity Models – A Collection. Available at: https://nataliehanson.com/2017/02/13/ux-maturity-models[195]
2. User-centred design toolkit. Available at: www.dpc.sa.gov.au/responsibilities/ict-digital-cyber-security/toolkits/user-centred-design-toolkit[196]

Accessibility

Action 2.11

The service provider partners with service users and their support people to:

a. Minimise barriers to accessing services associated with the hardware, software, data requirements and platform of the services, or the language, location, age, culture and ability of the service users and their support people
b. Ensure services are compatible with commonly used assistive technologies
c. Meet relevant standards for web page or web application
d. Regularly review access to services and take action to improve access by service users and their support people.

Intent of the action

Accessibility of the service is optimised for service users, taking account of the types of barriers that may affect access to the service.

Reflective questions

- What processes are in place to minimise barriers to access for service users?
- How does the service provider consider the language, location, age, culture and ability of the service users in the design and delivery of the service?
- Is the service compatible with commonly used assistive technologies?
- Does the service meet relevant national standards for webpages and web applications?
- How is the accessibility of the service measured and improved?

Meeting the action

Prioritise access and accessibility

Tasks for implementing the action:

- Endorse a policy that outlines accessibility as a central requirement for digital mental health services
- Review compliance with relevant standards for the platforms and formats used – for example, with Web Content Accessibility Guidelines (WCAG) 2.0 or 2.1 for web and app content
- Review the accessibility needs of intended user groups, including needs arising from disability, age, cultural diversity, language or location, and any potential barriers related to hardware, software, platform and data requirements
- Provide advice on the language and literacy proficiency required to use the digital mental health service to potential service users in the product information (Action 3.03)
- Provide information on the hardware, software, platform, and data requirements for service users.

Support access and accessibility

Tasks for implementing the action:

- Work with service users, consumers, carers, families and support people to understand the barriers that may impede their access to the service provider's digital mental health services, and work to remove them
- Undertake accessibility testing in the field as well as during development, and include testing with a wide variety of consumers and carers from the relevant service user group
- Develop a training package for the workforce that builds understanding of the diversity of service user needs and how service design can improve accessibility
- Periodically review the experience of service users in accessing the digital mental health service; use a survey, focus group or review of feedback and complaints, and take action to remedy any issues identified
- Undertake an audit against a reference standard, for example WCAG 2.1, or relevant legislation – for example, the *Disability Discrimination Act 1992* – to identify where and how the accessibility of digital mental health services could be improved.

An accessible website or app should provide text content that is readable and understandable and include options so that those with visual impairment or a text-only interface can still read the content of the website or app.

Content should be easy to hear (if applicable) and see, including separating the foreground from the background and making sure colours used are readable by users with colour blindness. If video or audio media is used, captions should be provided for those with hearing impairment or when it may not be appropriate to use audio settings (e.g. when being used in a shared space).

Content should be arranged such that users can change the formatting of the page without losing information. Users should be given time to read the content, or have the material dictated to them, without a web page timing out.

To prevent the risk of seizures, there should be no flashing lights or alternating colour backgrounds. If these exist, a warning should be provided and there should be an option to turn these settings off.

Assistive technologies seek to maintain or improve an individual's functioning and independence, encourage participation, and enhance overall wellbeing. They are used by individuals to perform tasks that might otherwise be difficult or impossible for them.

Compatibility with current and future assistive technologies should be supported. Common types of assistive technologies include:

- Computer access aids, voice-to-text software and modified keyboards
- Sensory aids for vision or hearing impairment, Braille and speech output devices and large print screens
- Other aids that assist people with speech and/or hearing disabilities to communicate.

Examples of evidence

Examples of evidence may include:

Information available to service users to promote access to the service provider's services
Results of audits of the service provider's services that reflect the accessibility of services to the intended users
Examples of assistive technologies available to the service users
Examples of compliance with relevant standards for web page or web application (e.g. WCAG 2.0 or 2.1)
Results of service user surveys about the accessibility of services, including from people with diverse disabilities
Feedback from service users about the accessibility of services and evidence of actions taken in response to feedback.

Related actions

This action relates to Action 2.10 (usability).

Useful resources

1. Web Content Accessibility Guidelines (WCAG) Overview. Available at: www.w3.org/WAI/standards-guidelines/wcag[197]
2. Assistive Technology Australia. Available at: https://at-aust.org/home/assistive_technology/assistive_technology[198]
3. A brief guide to the Disability Discrimination Act. Available at: https://humanrights.gov.au/our-work/disability-rights/brief-guide-disability-discrimination-act[199]
4. Online Accessibility Toolkit. Available at: www.accessibility.sa.gov.au[200]

Model of Care Standard

Service providers establish a model of care for each digital mental health service and implement and maintain systems to support the delivery of safe and high-quality care and to minimise the risk of harm to service users, their support people and others.

Intention of this standard

To ensure digital mental health services have a clearly defined model of care, consistent with best practice and evidence; and service users and, where relevant, their support people, receive care consistent with the model of care. The care provided aligns with the service user's expressed goals of care and healthcare needs and is clinically appropriate.

To ensure that risks of harm to service users are minimised and managed, including through the transition of care.

Criteria

Explanatory notes

Model of care

The model of care outlines the way a digital mental health service is to be delivered. Service users and their support people access digital mental health services through many channels and media, and the model of care for their chosen services may not always be obvious.

Service providers should understand and describe the purpose and intent of the service, how it is to operate, what it is intended to achieve and how it is informed by evidence and best practice. This can help to assist service users and, when relevant, their support people to make informed choices about digital mental health services.

The NSQDMH Standards apply to a wide variety of digital mental health services, and the actions in the Model of Care Standard may apply differently in each different type of service. Monitoring the delivery of care to ensure the service does what it promises to do, that it communicates clearly to the service user and engages with their support people (to the extent that the service user chooses) is equally necessary, but requires appropriate accountabilities to be put in place.

Minimising risk

Minimising risk in any care delivery setting is important. For digital mental health services, in-person interactions and environmental cues are often not available to signpost potential risks. Screening of risk is therefore important, especially when it comes to the risk of harm, including self-harm and suicide. If risk is detected, an effective response should be available, whether provided directly by the service or via referral to another agency.

Serious adverse events may be preceded by changes in a person's behaviour or mood that can indicate deterioration in their mental state. Early identification of deterioration may improve outcomes but can be more difficult in a digital setting. However, use of digital services should not mean a higher level of risk. A systematic approach to recognising deterioration early and responding to it appropriately is therefore required, noting that the response may include calling for emergency assistance internally or via external emergency response systems.

Communicating for safety

Communication is a key safety and quality issue, and no less so in services delivered digitally. Correct identification is an important component of communication in healthcare settings. When a service user is not physically present, it remains critical to ensure that they are correctly identified and receive continuity in their care, and that no other individual is able to inappropriately view their care details.

There are key times when effective communication and documentation are critical to the safety of service users and their support people. This includes when critical information about a service user's care emerges or changes, and when their care is transferred. Systems and processes should be in place to ensure effective communication at these times.

Criterion: Establishing the model of care

The service provider ensures that the model of care for each digital mental health service is goal-directed and can achieve the stated outcomes of care for service users and their support people.

Service providers determine the purpose and intent of the digital mental health service they provide, including the service users who can benefit most from the service. The model of care outlines the way the digital mental health service is to be delivered, based on the best available evidence and best practice. It should ensure that service users can exercise choice about the care options available to them to get the right care at the right time, including as they move through the stages of their mental health journey.

These goals will be best achieved through partnering with consumers, carers, families and support people in the design and development of the model of care.

Designing the model of care

Action 3.01

The service provider:

a. Documents the purpose and intent of the model of care for each service and the context in which it will operate
b. Defines the intended user demographic and matches the model of care to the service users and their support people
c. Monitors and evaluates the performance and effectiveness of the model of care
d. Assigns accountability for maintaining and improving the effectiveness of the model of care.

Intent of the action

The service provider has a model of care for each digital mental health service that enables and supports the delivery of care to service users.

Reflective questions

- How does the service provider document the model of care for each service, including outlining the intended users?
- What processes are in place to monitor and evaluate whether the models of care for each service are effective?
- What actions does the service provider take to update and improve the models of care of its services?

Meeting the action

The model of care describes the purpose and intent of the digital mental health service and broadly defines the way the service is organised and delivered. It considers the context of the digital mental health service, and the category of service that it aims to deliver, and outlines which interventions will be provided, when, how, to whom and for what purpose.

The model of care should:

- Be service user-centric
- Consider equity of access and new ways of organising and delivering care
- Support safe and high-quality care for service users
- Have a robust and standardised set of outcome measures and evaluation processes
- Link to local, state and national strategic plans and initiatives.

Design the model of care

The model of care should reflect the complexity of the intended service users' care needs and may differ between service users, settings and services. For example, a model of care for a service providing **information** about anxiety or depression may be simple, but a model of care for providing **treatment** of anxiety or depression may be more detailed.

Tasks for implementing the action:

- Clearly define the purpose and intent of the digital mental health service appropriate to the context in which it will operate

- Define the intended users of the digital mental health service, including any specific groups
- Work with clinicians, consumers, and carers to design, develop, document and communicate a model of care that accounts for specific settings, services or service user populations
- Plan systems for monitoring and evaluation early in the development of a model of care.

Implement the model of care

Work with clinicians and peer workers to agree on the content and use of care planning in the digital mental health service. Include the capacity to document service users' preferences and goals and individualise aspects of care as required. Ensure that the care to be delivered by the digital mental health service matches the care required and best meets the needs of the intended user group, as set out in the model of care.

Evaluate the model of care

A program logic describes the change process underlying an intervention and documents the connections between the critical components. It can help to identify what is important, identify outcomes and other effects of change, determine data collection sources and methods, select indicators and provide a mechanism for gaining cooperation and acceptability from stakeholders for monitoring.[201]

Tasks for implementing the action:

- Develop a program logic for the model of care that defines what should be measured and when
- Work with clinicians, service users and their support people to develop measures of the performance and effectiveness of the model of care; these may include the efficiency, impact and sustainability of the model of care
- Regularly monitor and evaluate the performance and effectiveness of the model of care using the agreed measures
- Assign clear accountability within the service provider for maintaining and improving the effectiveness of the model of care; use the performance and effectiveness data and other feedback.

Examples of evidence

Examples of evidence may include:

Documents that outline the model of care for each service, including the purpose of the service, the intended users, the outcomes expected, and the way in which the service is to work to achieve the stated purpose and outcomes for the intended audience
An audit of the adherence of the services delivered to the models of care
Analysis of variance data on the outcomes from use of each service against expected outcomes
Feedback from service users about whether the service met their expectations
Position descriptions that indicate accountability for the model of care of each service
Evidence of changes to the models of care of services based on an analysis of outcomes and feedback
Committee or meeting minutes that detail discussion about the models of care and any evaluation of or changes to the models of care.

Related actions

This action relates to Action 2.07 (partnering with service users in design of services).

Evidence supporting the model of care

Action 3.02

The service provider ensures the model of care for each service is based on best available evidence and best practice and supporting policies.

Intent of the action

The effectiveness of the digital mental health service is enhanced when the model of care reflects the best available evidence and best practice.

Reflective questions

- How does the service provider ensure the models of care for each service are based on evidence and reflect best practice?
- What processes are in place to ensure the models of care of its services are updated when the evidence base changes?

Meeting the action

The model of care should be guided by the best available evidence and outline best-practice care for the intended user group to ensure service users get the right care at the right time.

Identify the evidence base available and best practice

The best evidence available may include randomised controlled trials, qualitative research, expert opinion and scientific principles. Knowledge may also come from care delivered in non-digital settings and from audits, evaluations and quality improvement activities conducted by the service provider.

Tasks for implementing the action:

- Critically evaluate the relevant literature to understand the available evidence base, including what are considered best-practice interventions
- Use the available evidence, along with clinical expertise and service user values, to guide decisions about the development of the model of care
- Make clear to potential users through the product information (see Action 3.03) the nature of the evidence base, and follow the service provider's ethical principles to ensure the safety of users
- Analyse current digital mental health practices, including any innovations used nationally and internationally, and the outcomes and evaluation of these practices.

Review the evidence base

Periodically review the research evidence underpinning the model of care and the extent to which the model of care remains based on sound evidence and reflects best practice. Make changes as necessary to incorporate the most recent findings into the model of care.

Build the evidence base through research or evaluation of the digital mental health services. When appropriate, share these findings with service users and publish them in the scientific literature.

Regularly update the model of care based on new research and evidence.

Examples of evidence

Examples of evidence may include:

Literature searches that show the evidence relied upon by the model of care at the time of development of each service

Clinical guidelines that set out best practice for the services being delivered

An audit of the alignment of the model of care for a service with the available evidence and best practice

Research trials or other scientific endeavours that evaluate a service and comment on its evidence base or practice

Consumer-led research and evaluation of the experience and outcomes of the model of care

Endorsement by professional associations or academic institutions that the model of care of a service reflects the evidence base or contemporary practice

Systems to periodically review and update the evidence base that underpins the model of care and to report on the implications of new evidence for the model of care

Expert opinions about the contemporary nature of the model of service and any required changes

Committee or meeting minutes that detail discussions about updates to the model of care based on updated evidence.

Useful resources

1. Evidence Standards Framework for Digital Health Technologies. Available at: www.nice.org.uk/Media/Default/About/what-we-do/our-programmes/evidence-standards-framework/digital-evidence-standards-framework.pdf[202]

Information for service users

Action 3.03

The service provider provides product information on each service to service users and, where relevant, their support people that:

a. Aligns with the current template endorsed by the Australian Commission on Safety and Quality in Health Care

b. Is easy to understand and meets their needs.

Intent of the action

The service user has the information they need to make an informed choice about whether to use a digital mental health service.

Reflective questions

- Does the service provider provide concise and easy-to-understand product information about each service to service users?
- How does the service provider assess whether the information in the product information meets the needs of diverse service users?

Meeting the action

To make an informed choice about whether to use a digital mental health service, consumers require information about the service. The Australian Commission on Safety and Quality in Health Care has developed a template for product information covering seven key domains. It is available at www.safetyandquality.gov.au/publications-and-resources/resource-library/product-information-template-digital-mental-health-services.

Use of the template is not mandatory and service providers may provide information about their digital mental health service in other ways – for example, via their website. However, service providers must make this information easy for consumers, carers and families to locate and understand.

Develop product information

Engage with service users to co-design the product information.

Endorse a policy on the provision of product information to service users; include the:

- Format to be used
- Methodology for disseminating the product information
- Frequency of review of the product information
- Triggers for an early review or update.

Publish product information

Tasks for implementing the action:

- Publish product information in an accessible format appropriate to the intended user group, using contemporary knowledge about preferred communication methods of different age groups
- Ensure that plain English is used so the product information is easy to understand
- Make alternative formats available to meet the diverse needs of users – formats could include large print, audio, pictorial, translated or suitable for screen readers, and other assistive technologies

- Consider other options for sharing product information – for example, telephone-based services may make product information also available via web, email or SMS
- Highlight the product information to ensure that service users understand where the product information is located and the importance of reading it before making decisions about their care
- Allow service users to seek further clarification, if required, or to acknowledge they have read the product information as part of the terms and conditions of the service.

Review the product information

Periodically survey service users' views on the content, language and format of the product information. Use feedback and complaints received to update the product information.

Periodically review the product information to ensure that it remains up to date and reflects any updates to the digital mental health service.

Examples of evidence

Examples of evidence may include:

A policy on the development and provision of product information to be provided to service users; the policy should:

- align with the current template
- set out the requirements for different languages and formats, consistent with the intended users

Product information for each service

Feedback from (or survey of) service users on the product information provided for a service, especially on whether it is easy to understand and meets their needs

Evidence of updates to product information in line with changes to the model of care or changes in legislation.

Useful resources

1. Product information template. Available at: www.safetyandquality.gov.au/publications-and-resources/resource-library/product-information-template-digital-mental-health-services[203]

Criterion: Delivering the model of care

The care delivered is consistent with the model of care and provided in partnership with service users and, where relevant, their support people.

Delivering the model of care

Action 3.04

The service provider:

a. Monitors the delivery of their service to ensure it is consistent with the model of care
b. Has a process for assigning responsibilities to a member of the workforce for the overall accountability of the care of each service user
c. Develops the goals of care and actions for treatment in partnership with the service user
d. Clearly communicates the care plan to the service user
e. Enables the involvement of support people, to the extent that the user chooses
f. Has a process for referral to follow-up services that is consistent with the model of care.

Intent of the action

Safe and effective care is delivered in line with the model of care and the service user's needs and preferences, and the outcomes of care are reviewed regularly to ensure that the goals of care are being met.

Reflective questions

- How does the service provider monitor the delivery of services?
- What processes does the service provider have to ensure that there is one person with overall accountability for the care of each service user?
- What processes are in place for when the service user stops receiving care from a service?

Meeting the action

Monitor the delivery of care

Tasks for implementing the action:

- Establish systems to ensure that the digital mental health service delivers care in line with the model of care
- Establish systems for service users and, when relevant, their support people to provide feedback about the model of care and the process of care delivery.

Develop the care plan

The care plan includes the goals of care and the actions to be taken to achieve them, actions required to manage identified risks of harm, indications for review of the care plan, and, if applicable, the process for referral to follow-up services. Goals of care should be recovery-orientated and person-centred.

Tasks for implementing the action:

- Work with the service user and, if appropriate, their support people to decide on the goals of care; they may be:
  - condition-specific – for example, to complete cognitive behaviour therapy homework
  - functional – for example, to continue to travel on public transport independently
  - personal – for example, to attend their daughter's wedding in four weeks
- Tune the level of detail in the care plan to reflect the nature and complexity of the digital mental health service.

Communicate the care plan

Tasks for implementing the action:

- Provide service users with a copy of their care plan using a secure means appropriate to the nature of the digital mental health service and the service user's preference
- Support ongoing communication between the service provider and the service user about the plan for their care and their progress in achieving their goals
- Determine what information and how often communication should occur in conjunction with the service user to build a shared understanding and enhanced trust.

Identify support people

Tasks for implementing the action:

- Give service users choice about when and how to let carers, families and support people be involved in their care and decision-making
- During engagement with the digital mental health service, ask the service user to identify any support people they wish to be involved in communications and decision-making about their care
- Allow the service user to nominate or change their nominated support people at any time throughout their care.

Plan follow-up care

Part of the care planning process is planning for when the service user no longer engages with the digital mental health service, including whether any follow-up may be needed.

Tasks for implementing the action:

- Engage early with the service user and, when appropriate, their support people in planning for when the service user no longer engages with the digital mental health service
- Develop processes to ensure that any referrals required for follow-up care are dealt with promptly.

Review the care plan

Tasks for implementing the action:

- Document service user progress against the goals of care
- Regularly reassess a service user's care needs, preferences and goals, and revise their care plan as necessary
- Review the care plan when important events occur – for example:

  - after critical events such as self-harm
  - when the service user or their support people request it or express concerns
  - if the service user does not reach a planned goal within a predetermined time or experiences no improvement after a period of treatment.

Provide education and training

Tasks for implementing the action:

- Provide orientation, education and training for members of the workforce so that they understand their roles, responsibilities and accountabilities in delivering care in line with the care plan
- Provide guidance to the workforce and service users about the need for the care plan to be developed in collaboration with service users and, when relevant, their support people
- Support the workforce to use shared decision-making processes in the context of planning and delivering digital mental health care.

Involve service users and their support people

Tasks for implementing the action:

- Work in partnership with service users and their support people when delivering care
- Ensure that collaboration with support people is effective, and in line with the preferences and consent of individual service users
- Recognise and document any special circumstances of the service user's support people – for example, when they may be the legal guardian of the service user or when they live in the same house as the service user and may be directly or indirectly affected by a care plan
- Consider ways to make engagement with service users and their support people trauma-informed and culturally appropriate.

Review processes

Tasks for implementing the action:

- Involve service users and the workforce in reviewing the effectiveness and usefulness of care delivery processes
- Develop processes for ensuring that updates and changes to care planning tools and processes are effectively communicated to the workforce.

Set up processes for identifying the clinician with overall accountability

Tasks for implementing the action:

- Allocate overall accountability for an individual service user's care to one member of the workforce to lead and coordinate care planning and delivery, and ensure that they are accessible and available as required
- Develop processes for identifying the person with accountability for each service user's care.

Examples of evidence

Examples of evidence may include:

Policy documents that outline processes for the delivery of the service that are consistent with the model of care and also require that overall accountability for each service user be assigned to a designated member of the workforce

Audits of the fidelity to the model of care of the service delivered

An audit of healthcare records that indicates that each service user has a designated individual with overall accountability for their care

A survey of service users about their experience of the service, including whether goals of care and actions for treatment were developed in partnership and clearly communicated to them

A policy document that outlines the processes that support the involvement of service users' support people in communications and decision-making

Healthcare records that document the involvement of support people in communications and decision-making

A standardised template for referral to follow-up services or evidence of completed referrals.

Related actions

This action relates to Action 2.04 (planning care).

Criterion: Minimising harm

In line with the model of care, service users at risk of harm are identified and targeted strategies are used to prevent and manage harm to service users or others.

Screening actions aim to identify the service users who are at the greatest risk of harm while receiving digital mental health care. Implementing targeted, best-practice strategies can prevent or minimise the risk of harm.

Screening of risk

Action 3.05

The service provider has systems to identify service users who are at risk of harm, including self-harm and suicide.

Intent of the action

Service users receive prompt screening and, when indicated, assessment and identification of risk.

Reflective questions

- How does the service provider identify service users who are at risk?
- What are the potential risks that users of this service are most likely to face?

Meeting the action

Develop screening processes

Tasks for implementing the action:

- Develop screening processes to identify:
  - existing conditions or issues that may predispose a service user to further harm
  - the likelihood that potential new harms occur
- Identify the diversity of the intended user group(s) served by the digital mental health service provider and the conditions and risks likely to be encountered
- Work with clinicians, consumers, carers, families and support people to develop screening and assessment processes

that are appropriate to the needs of service users and the digital mental health services being provided

- Ensure that the risks of harm from self-harm and suicide, and risk of harm to others or from others, are addressed in these processes.

Implementing screening processes

The conditions, issues and risks identified through screening must be properly assessed to work out what actions should be taken to manage them. Processes may vary for different groups of service users and in different digital mental health services.

Tasks for implementing the action:

- Develop policies, procedures and protocols that set out the expectations about the timing of a first screening, the assessments and actions to take when risks of harm are identified, and the indications for repeated screening and assessment
- Work with clinicians and peer workers to integrate screening processes into the workflow of the digital mental health service
- Develop information about screening processes to include in orientation, education, and training programs for the workforce
- Develop processes for ensuring that updates and changes to screening tools and processes are effectively communicated to all stakeholders.

Evaluation of screening processes

Tasks for implementing the action:

- Periodically review feedback from quality improvement processes relevant to screening and assessment
- Involve the workforce and service users in reviewing the effectiveness, usability and usefulness of screening processes.

Use tools and resources

Use published guidance, tools and resources about suicide prevention strategies and how to implement them (see **Useful resources** below).

Examples of evidence

Examples of evidence may include:

Policy documents that outline processes for how services can conduct screening, including:

- when routine screening of service users will occur
- the roles and responsibilities of members of the workforce when service users are routinely screened
- the process for taking action when risks are identified
- indications for repeating the screening process

Observation of practice that shows use of relevant screening processes

Records of interviews with the workforce that show that they understand the service provider's screening processes and their responsibilities

Training documents about screening processes

Communication with the workforce about updates to screening processes

Results of audits of healthcare records of screening

Feedback from service users about screening

Assessment of the risks relevant to the population serviced by the service

Resources and tools developed by the service provider for screening and assessment of clinical conditions and risks that are relevant to the service provided

Training documents about the identification and assessment of at-risk service users.

Related actions

This action relates to Action 3.06 (planning for safety), Action 3.11 (escalating care) and Action 3.12 (responding to acute deterioration).

Useful resources

1. The National Aboriginal and Torres Strait Islander Suicide Prevention Strategy. Available at: www.health.gov.au/resources/publications/national-aboriginal-and-torres-strait-islander-suicide-prevention-strategy[204]
2. Suicidal Signs to Look for in Someone. Available at: www.beyondblue.org.au/the-facts/suicide-prevention/worried-about-someone-suicidal/suicidal-signs-to-look-for-in-someone[205]
3. Recognising Suicide Warning Signs. Available at: www.suicideline.org.au/worried-about-someone/recognising-suicide-warning-signs[206]
4. Suicide risk assessment questions. Available at: www.square.org.au/risk-assessment/risk-assessment-questions[207]
5. Lifeline suicide data and statistics. Available at: www.lifeline.org.au/resources/data-and-statistics[208]
6. SOARS Model: Risk assessment of nonsuicidal self-injury: Available at: www.contemporarypediatrics.com/view/soars-model-risk-assessment-nonsuicidal-self-injury[209]

Planning for safety

Action 3.06

The service provider has systems to:

a. Effectively respond to service users who are distressed, have expressed thoughts of self-harm or suicide, or have self-harmed
b. Effectively respond to service users who present a risk of harm to others
c. Provide information to service users with healthcare needs beyond the scope of the service on where and how to access services appropriate to their clinical need
d. Enable crisis intervention aligned to legislation.

Intent of the action

Adverse outcomes relating to service users who are distressed or have thoughts of self-harm or suicide or who have self-harmed are prevented through early recognition and effective response.

Reflective questions

- How does the service provider respond to service users who are distressed, have expressed thoughts of self-harm or suicide, or have self-harmed?
- What referral processes does the service provider have in place?

Meeting the action

Assess the risk

Tasks for implementing the action:

- Communicate with the service user, their support people, and others respectfully and in non-judgemental language to create safety in the digital setting and avoid making presumptions about their intent
- Develop processes to assess the risk of service users who are distressed, have thoughts of self-harm or suicide, or have self-harmed
- Set up a system for response according to the level of risk.

Responding to risk of self-harm

Self-harm can be related to suicidal thoughts or can be independent of these. The service user may or may not be clear about their intent. Some self-harm may be enacted without suicidal ideation, but still present a risk to the person's life. Always consider self-harm seriously.

Develop options for escalating care when a service user discloses a risk of self-harm or has self-harmed, including referring to a senior clinician or peer worker internally or referring to an appropriate external service.

Responding to risk of suicide

Tasks for implementing the action:

- Develop options for escalating care when a service user discloses suicidal thoughts or has attempted suicide – options include

referring to a senior clinician or peer worker internally and referring to an appropriate external service, including an emergency service if a crisis response is needed

- Develop options for providing after-care to service users who have experienced a suicidal crisis or a suicide attempt; options may be within the service provider's digital mental health services or provided by an external after-care service
- Develop options for providing care and assistance to the support people of a service user who is experiencing a suicidal crisis, a suicide attempt or who has died by suicide; the service provider may provide these services or have options for referring to a partner organisation to do so
- Use a recovery-orientated approach, focused on restoring hope through engagement with a service user after a suicide attempt
- Consider the needs of support people after a service user's suicide attempt.

Responding to risk of harm to others

Alcohol and other drug use and mental health difficulties may increase risk of harm to others.[210] Develop a system to respond appropriately if a service user discloses thoughts of harm to others or if they are assessed as representing a risk to others. This may include referring the service user to a specialist mental health service for assessment or to an emergency service if a crisis response is needed.

Develop procedures on the response required when there is risk of harm or neglect to children, including when a notification to child welfare or a referral to family support services is indicated.

Responding to risk of harm from others

Service providers should consider whether a service user may be at risk of experiencing harm from others. The level of risk may be increased by factors such as alcohol or drug use, disinhibition and other risk-taking behaviours, domestic and family violence, intimate partner violence, child abuse and neglect.[211,212]

Develop a system to respond appropriately to service users who are at risk of harm from others. The system may include escalating care to a senior clinician or peer worker internally or referring to external specialist services, including to an emergency service if a crisis response is needed.

Describe response processes

Develop information about response processes, including information about when crisis intervention is enabled by legislation, and make this information available to service users, their support people and the workforce.

Clearly set out the circumstances in which confidential information about the service user may be disclosed without their consent when responding to risk of harm to themselves or others.

Train the workforce

Tasks for implementing the action:

- Ensure members of the workforce understand the importance of being transparent with service users and their support people about the limits of confidentiality and when emergency services will be called
- Provide training to the workforce on how to support service users if their confidentiality has had to be breached
- Provide training to the workforce on ways to engage effectively with support people when a service user is at risk.

Review responses to risk

Tasks for implementing the action:

- Review the effectiveness of escalation and response processes regularly, as well as in response to critical incidents
- Develop strategies and processes for the workforce and service users to provide feedback about the usability and effectiveness of response processes.

Examples of evidence

Examples of evidence may include:

Policy documents that outline collaborative processes for identifying and treating service users at risk of self-harm or suicide, or who have self-harmed

Risk assessment tools for service users at risk of self-harm or suicide

Training documents about identifying and treating service users at risk of self-harm or suicide, or who have self-harmed

Service user information packages or resources about strategies for managing self-harm, or risks of self-harm or suicide, and escalation protocols

A clinical incident monitoring system that includes information on self-harm and suicide

Resources for the workforce to help identify service users who require close monitoring

Service user experience surveys, a complaints management system and a service user participation policy for service users at risk of self-harm or suicide

Observations that information about referring service users to specialist mental health services is accessible to the workforce.

Useful resources

1. Care After a Suicide Attempt. Available at: www.blackdoginstitute.org.au/wp-content/uploads/2020/04/careafterasuicideattempt02-09-15.pdf[213]
2. Assessment and management of risk to others. Available at: www.rcpsych.ac.uk/docs/default-source/members/supporting-you/managing-and-assessing-risk/assessmentandmanagementrisktoothers.pdf[210]
3. Abuse and Violence. Appendix 1: Nine steps to intervention. Available at: www.racgp.org.au/clinical-resources/clinical-guidelines/key-racgp-guidelines/view-all-racgp-guidelines/white-book/appendices/appendix-1-nine-steps-to-intervention-the-9-rs[214]
4. Clinical Practice Guideline for the management of Borderline Personality Disorder. Available at: www.nhmrc.gov.au/about-us/publications/clinical-practice-guideline-borderline-personality-disorder[215]

Criterion: Communicating for safety

Service providers have systems in place for effective and coordinated communication that supports the delivery of safe and high-quality care for service users and their support people.

In a digital mental health service, processes to match service users to their intended care are critical to ensuring users' privacy and safety. A comprehensive system to reliably identify the service user at each contact allows the service user to be matched to their intended care. Service users may choose to use an alias or to access services anonymously, but matching them to their intended care can still occur.

Critical information can arise at any point during a service user's engagement with a digital mental health service and may come from many sources, including the service user or their support people. What information is critical may differ depending on the type of digital mental health service. Service providers must consider and define what is critical information for the digital mental health services they offer, and have in place formal processes to ensure that critical information is appropriately communicated whenever it emerges or changes.

Planning for when a service user no longer engages with a digital mental health service requires consideration of the significance and complexity of the service user's health issues, their risk of harm, and their ongoing mental health needs.

Correct identification

Action 3.07

The service provider has processes to:

a. Routinely ask if a service user is of Aboriginal and/or Torres Strait Islander origin, and to record this information in administrative and clinical information systems

b. Authenticate service users and match them to their care

c. Protect the anonymity of the service users where this is part of the model of care

d. Use appropriate identifiers for service users according to digital services best-practice guidelines.

Intent of the action

Service users are correctly identified and matched to their care, and their anonymity is preserved if applicable. Service users who identify as of Aboriginal and/or Torres Strait Islander origin and who wish to have their cultural identity recorded can do so to inform the development and delivery of culturally safe digital mental health care.

Reflective questions

- What processes are in place to ask if service users wish to record that they identify as Aboriginal and/or Torres Strait Islander?
- How is this information recorded in administrative information systems and transferred to clinical information systems?
- What processes are in place to ensure that service users are correctly identified and matched to their care?
- If the service is provided anonymously, how does the service provider protect the anonymity of the service user?

Meeting the action

Develop a service user identification system

Develop policies, procedures and protocols that ensure the consistent and correct identification of a service user at any time during their engagement with the digital mental health service. The type of service user identification and matching process will depend on the type of digital mental health service, the model of care and the risks for the service user.

Specify in the policy, procedures and protocols the number and types of service user identifiers (such as name, date of birth, gender, email, password, address, postcode, healthcare record number, Individual Healthcare Identifier) that will be used to identify a service user when digital mental health services are provided, including:

- On registration with the digital mental health service
- When matching a service user's identity to services
- Whenever handover or transfer of care occurs
- Whenever documentation is generated.

Require the national unique Individual Healthcare Identifier to be included as a service user identifier wherever the My Health Record system is in use (see Action 1.17).

Refer to best practice for digital services when defining the approved service user identifiers for use in the digital mental health service.

Train the workforce to build competence in working with diverse population groups and collecting identification information. This may also include training in cultural safety.

Anonymous service users

Tasks for implementing the action:

- Specify in the service user identification policy what service user identification will be used to match the service user to their treatment and protect their safety when the model of care provides for the digital mental health service to be accessed anonymously
- Ensure that the service user's anonymity will be protected by the service user identification methods that are chosen.

Identify Aboriginal and Torres Strait Islander service users

The availability of processes for the correct and consistent identification and recording of Aboriginal and Torres Strait Islander service users is important for upholding the rights and meeting the needs of these service users. Collection of these data should only occur when a service provider has established a commitment to using the data for better service planning for Aboriginal and Torres Strait Islander peoples or improving service delivery.

Tasks for implementing the action:

- Develop policies, procedures and protocols on Aboriginal or Torres Strait Islander identification that respect the service users' wishes
- Partner with Aboriginal and Torres Strait Islander service providers, elders or communities to design and improve the service provider's processes for Aboriginal and Torres Strait Islander identification
- Develop resources in formats that are easily accessible for Aboriginal and Torres Strait Islander service users to explain why the question of Aboriginal and Torres Strait Islander identity is being asked
- Work in collaboration with Aboriginal and Torres Strait Islander organisations to train and support the workforce to collect identification information in a culturally appropriate way
- Establish mechanisms to improve cultural competency and reflective practice of the workforce to improve the willingness of Aboriginal and Torres Strait Island people to identify
- Use the confirmation of a service user as being of Aboriginal or Torres Strait Islander origin to provide culturally appropriate care, including the use of an Aboriginal Health Worker or interpreter if required, and better assessment of the risks they may face
- Include Aboriginal and Torres Strait Islander identifiers in administrative and clinical datasets
- Ensure that, when Aboriginal or Torres Strait Islander identity is established through an administrative process, there are mechanisms to transfer it to the service user's healthcare record
- Monitor trends in the delivery and outcomes for Aboriginal and Torres Strait Islander users of digital mental health services to inform improvement strategies for service delivery to Aboriginal and Torres Strait Islander peoples
- Monitor and report on the implementation of Aboriginal and Torres Strait Islander identification strategies.

Identify other diverse populations

Service providers may wish to apply an approach for identification for individuals from culturally and linguistically diverse and LGBTIQ+ backgrounds when digital mental health service provision to this group has been identified by the service provider as a priority.

Examples of evidence

Examples of evidence may include:

A policy document that describes the service provider's requirements for the identification and authentication of service users (in line with the model of care) and includes:

- processes for asking if service users are Aboriginal and/or Torres Strait Islander
- processes for recording this information in administrative and clinical information systems
- methods to match service users to their care following identification and authentication
- approaches that protect the anonymity of service users when this is part of the model of care or requested by the service user
- use of appropriate identifiers according to digital services best-practice guidelines

A registration form on which service users can identify as being of Aboriginal or Torres Strait Islander origin

Communication material that provides service users with information about why they will be asked if they are of Aboriginal or Torres Strait Islander origin

Training or contract documents about obtaining information about Aboriginal and Torres Strait Islander service users

Communication with the workforce about the importance of identifying Aboriginal and Torres Strait Islander service users

Analysis of incidents relating to failure to correctly identify or authenticate service users or to match them to their care, and any associated actions to be implemented as a result

Analysis of incidents about failure to protect the anonymity of service users and any associated actions to be implemented as a result

Observation of system for using appropriate identifiers for service users.

Related actions

This action relates to Action 1.20 (cultural awareness and competence).

Useful resources

1. National best practice guidelines for collecting Indigenous status in health data sets. Available at: www.aihw.gov.au/reports/indigenous-australians/national-guidelines-collecting-health-data-sets/summary[216]
2. Australian Bureau of Statistics Indigenous Status Standard. Available at: www.abs.gov.au/statistics/standards/indigenous-status-standard/latest-release[217]
3. Cultural Respect Framework 2016–2026 for Aboriginal and Torres Strait Islander Health: A national approach to building a culturally respectful health system. Available at: www.coaghealthcouncil.gov.au/Portals/0/National%20Cultural%20Respect%20Framework%20for%20Aboriginal%20and%20Torres%20Strait%20Islander%20Health%202016_2026_2.pdf[23]
4. Guidelines for System Hardening. Available at: www.cyber.gov.au/acsc/view-all-content/advice/guidelines-system-hardening[116]
5. One simple question could help you close the gap. Available at: www.aihw.gov.au/getmedia/502680f6-b179-42fa-be71-8fd5d793d8d8/indigenous-identification-DLbrochure.pdf.aspx[218]

Communication of critical information

Action 3.08

The service provider has processes to:

a. Communicate when critical information about a service user's care emerges or changes, to ensure the safety of the user

b. Enable service users and their support people to communicate critical information and information on risks to their service provider.

Intent of the action

Emerging or new critical information, alerts and risks are communicated in a timely manner, including by service users and their support people.

Reflective questions

- How does the service provider communicate critical information to protect the safety of service users?
- Are service users able to communicate information about risks to the service provider?

Meeting the action

Identify critical information

To identify critical information, it must first be defined. Define 'critical information' in the context of the service provider's digital mental health services, considering factors including the nature of the digital mental health service and the needs of the intended user group. Types of critical information could include:

- Change in service user goals
- Change in service user circumstances
- Change in service user mental state
- Change to service user medicines
- Allergies or adverse drug reactions
- Information that requires follow-up with another clinician or the service user (or their support people, if appropriate)
- Incorrect diagnosis or change in diagnosis.

Identify situations when communication of critical information is required

Tasks for implementing the action:

- Identify when and to whom communication of critical information, alerts or risks should occur, including communication with service users and support people
- Review or map the service provider's current critical information communication processes
- Analyse work processes that require critical information to be shared inside and outside the organisation
- Collect baseline data about the critical information communication issues and needs of the organisation by interviewing, surveying or observing the workforce and service users; find out:
  - the details of gaps and issues
  - whether the workforce and service users are aware of existing communication processes
  - whether they are using them

- Perform a risk assessment to reveal areas for improvement in relation to critical information communication gaps and areas of good practice
- Revise or develop policies and processes to reduce identified gaps.

Review policies for communicating critical information

Tasks for implementing the action:

- Review the service provider's policies and processes to find out whether they support and enable effective communication of critical information
- Ensure that policies and processes clearly define:
  - the types of critical information that must be communicated
  - when communication should occur, including flags, triggers, alerts and other criteria
  - the method for communicating critical information to the responsible clinician
  - the method for communicating critical information to the service user or support people (if appropriate)
  - the expected time frames for this communication
  - how to escalate in the event of no response
  - how the information is documented, including the actions taken in response to the critical information to ensure service user safety
  - whether open disclosure is relevant
- Revise policies and processes to fill any identified gaps in collaboration with the workforce, service users and support people to ensure that policies are user-centred and meet the needs of the people involved.

Support closed-loop communication in developing processes so the person who is communicating the information knows that the message has been received, and there is a response that lets them know that action will be taken to deal with the communication need.[219] Closed-loop communication is especially important if communication occurs through tools or technologies that do not allow two-way communication.

Provide resources and tools to aid effective communication processes

Tasks for implementing the action:

- Establish agreed communication processes and pathways to ensure that members of the workforce are clear about who to communicate new critical information to, and who is responsible for the action or follow-up
- Educate, train and support all members of the workforce, including non-clinicians who may communicate with service users, about the policies, processes, resources and tools for communicating critical information and use of these tools, and their responsibilities to effectively communicate in key high-risk situations
- Provide information about resources and tools for communicating critical information to service users and support people, and periodically review whether this support is meeting the needs of service users and their support people.

Examples of evidence

Examples of evidence may include:

A review of process mapping that identifies the situations in which communication of emerging or changing critical information are required

A risk register that includes identified risks for receipt and distribution of critical information to responsible clinicians

Activities to manage identified risks with receipt and distribution of critical information

Reports, investigations and feedback from the incident management and investigation system that identifies incidents relating to receipt and distribution of critical information

Documented processes for communicating critical information when there is an unexpected change in a service user's status or when new critical information becomes available

Policy documents that outline the:

- types of critical information that are likely to be received, and actions to be taken in response
- method for communicating critical information to the responsible clinician
- method for communicating critical information to the service user and their support people
- time frames for communicating critical information

Results of audits of workforce compliance with policies relating to communicating critical information

Examples of information provided to patients, carers and families about processes for communicating concerns to the clinicians responsible for care.

Related actions

This action relates to Actions 2.05 and 2.06 (communication that supports effective partnerships) and Actions 3.10 and 3.12 (recognising and responding to acute deterioration).

Useful resources

1. Clinical Communication and Teamwork. Available at: https://www.sahealth.sa.gov.au/wps/wcm/connect/Public+Content/SA+Health+Internet/Clinical+Resources/Clinical+Programs+and+Practice+Guidelines/Safety+and+Wellbeing/Communicating+for+safety/Clinical+handover+and+teamwork[220]
2. Communication Tools – UCLA Health. Available at: www.uclahealth.org/nursing/workfiles/CompetenciesEducation/LP-Saftey-CommunicationSkills.pdf[221]
3. TeamSTEPPS Fundamentals Course: Module 3. Communication. Available at: www.ahrq.gov/teamstepps/instructor/fundamentals/module3/igcommunication.html[222]
4. Communication Skills: A guide to practice for healthcare professionals. Available at: www.ausmed.com.au/cpd/guides/communication-skills[223]

Transfer of care

Action 3.09

The service provider:

a. Has processes to effectively communicate when all or part of a service user's care is transferred
b. Determines minimum information content to be communicated when care is transferred
c. Sets out the process for a transfer of care, in line with the model of care
d. Assesses risks relevant to the service's context and the particular needs of the service user when a transfer of care occurs
e. Encourages service users and, where relevant, their support people to be involved in the transfer of their care.

Intent of the action

Service users' safety and care is maintained by accurate and relevant communication when care is transferred.

Reflective questions

- What processes are in place to transfer the care of the service user at the end of their care?
- How does the service provider assess the service user's needs and risk at the point of transfer of care and ensure effective communication occurs to support the transfer of care?

Meeting the action

Plan ahead

Tasks for implementing the action:

- Develop policies and procedures that require proactive planning to be routine when a service user no longer engages with a digital mental health service; include a process for transfer of care when this is required
- Ensure that the significance and complexity of the service user's health issues and risks of harm are considered and balanced with the service user's stated preferences for their ongoing care
- Use the principles of shared decision-making when collaboratively developing the plan to meet the service user's ongoing mental health needs
- Clearly communicate the transfer-of-care policies and processes to the workforce, including expectations for using the processes.

Define the minimum information content

Collaborate with clinicians, peer workers, service users and support people to define the minimum information content to be communicated when care is transferred. Consider the type of digital mental health service and the situation in which transfer of care is occurring.

Provide guidance to the workforce and service users and their support people to ensure that all participants involved in a transfer of care are aware of what the minimum information content is, and their roles and responsibilities for communicating and receiving this information.

Implement the process

Tasks for implementing the action:

- Involve service users and their support people as key participants in the transfer of care, if possible
- Maintain the service user's privacy and confidentiality during transfer of care
- Use interpreters as required in the development and communication of the plan for transition of care; if English is not the first language of the service user, ensure that they and their support people understand the plan and (if relevant) who their ongoing care providers are
- Communicate the plan, using appropriate means (which may include verbal, written and digital means) and ensure that those involved in any transfer-of-care process are aware of their roles and responsibilities and the service user's goals and preferences.

Support the workforce

Tasks for implementing the action:

- Provide orientation and training to support the workforce, service users and support people in planning and implementing transfer of care and in the use of tools for transferring the service user's care and information correctly
- Provide access to structured tools to support the transfer of care.

Examples of evidence

Examples of evidence may include:

A model of care that documents the options for transfer of care

Policy documents that specify the risk assessment process and the minimum information to be communicated at transfer of care

Evidence that clinicians were involved in specifying the minimum information to be communicated at transfer of care

Feedback from the workforce on the use of transfer-of-care policies, procedures and protocols

Observation of clinicians' practice that shows use of structured risk assessment and communication processes and tools at transfer of care

Records of interviews with clinicians that show that they understand the service provider's structured processes for transfer of care

Results of audits of completed documentation that show effective handover of responsibility for care; documents may include standardised transfer forms, completed transfer forms and standardised referral letters

Results of audits of workforce compliance with transfer-of-care policies, procedures and protocols

Training documents about responsibilities and processes for transfer of care
Communication with the workforce about transfer-of-care processes
Information provided to service users that outlines their role in the transfer of care, such as a charter of rights or service user information sheet
Results of a service user experience survey, and service user feedback about transfer of care
Results from workforce satisfaction surveys and feedback about referral and use of transfer-of-care processes.

Related actions

This action relates to Action 2.04 (planning care) and Action 3.04 (delivering the model of care).

Useful resources

1. iSoBAR (Identify, Situation, Observations, Background, Agree to a plan, Readback). Available at: https://doi.org/10.5694/j.1326-5377.2009.tb02625.x[224]
2. ISBAR (Identify, Situation, Background, Assessment, Recommendation). Available at: https://doi.org/10.1186/s12909-020-02285-0[225]
3. SBAR (Situation, Background, Assessment, Recommendation). Available at: www.ihi.org/resources/Pages/Tools/sbartoolkit.aspx[226]
4. SHARED (Situation, History, Assessment, Risk, Expectation, Documentation). Available at: www.safetyandquality.gov.au/sites/default/files/2019-06/shared_resource_guide.pdf[227]
5. Implementation Toolkit for Clinical Handover Improvement. Available at: www.safetyandquality.gov.au/our-work/communicating-safety/clinical-handover/implementation-toolkit-clinical-handover-improvement[228]
6. OSSIE Guide to Clinical Handover Improvement. Available at: www.safetyandquality.gov.au/our-work/communicating-safety/clinical-handover/ossie-guide-clinical-handover-improvement[229]
7. CUSP Toolkit – Implement teamwork and Communication Module. Available at: www.ahrq.gov/hai/cusp/modules/implement/index.html[230]
8. Safe Communication: Design, implement and measure – A guide to improving transfers of care and handover. Available at: www.england.nhs.uk/signuptosafety/wp-content/uploads/sites/16/2015/09/safe-comms-design-implmnt-meas.pdf[231]

Criterion: Recognising and responding to acute deterioration

Acute deterioration may occur at any time during a service user's engagement with a digital mental health service. Tracking changes in mental state over time plays an important role in detecting acute deterioration. If monitoring is intermittent or infrequent, or does not include the right parameters, acute deterioration may not be detected, and recognition and appropriate treatment may be delayed. This can result in serious adverse outcomes for service users.

Recognising acute deterioration relies on detecting, understanding and interpreting abnormal mental state signs and other observations. This may be more difficult in a digital environment. A systematic approach can help to ensure that signs for detecting deterioration in a service user's mental state are being monitored. Training of the workforce is important to support best functioning of systems for recognising and responding to acute deterioration.

Recognition systems also include identifying the requirements for escalating care. These may be documented in policies and guidelines, and in escalation protocols that provide details of the defined parameters and thresholds that indicate acute deterioration, the action to be taken when deterioration is detected, the process of calling for help and the expected responses.

Escalation protocols are developed in line with the model of care of the digital mental health service. Criteria for escalation appropriate for one digital mental health service may not be appropriate for another. The availability of resources and clinical expertise also means that responses may vary from one service provider to another.

In addition, response systems must be in place. Response systems ensure that all patients who acutely deteriorate receive a quick and appropriate response.

Recognising acute deterioration

Action 3.10

The service provider uses defined parameters to recognise acute deterioration in mental state that requires care to be escalated.

Intent of the action

Service users with acute deterioration are identified early and adverse outcomes relating to acute deterioration in a person's mental state are prevented through early recognition and effective response.

Reflective questions

- What processes are in place to detect deterioration in the service user's mental state?

Meeting the action

Be alert for signs of deterioration in a service user's mental state

Work with service users and clinical and peer worker groups to agree on parameters for acute deterioration that requires escalation of care. These parameters may be based on mental state examination, frequency of contact, or other key elements.

Tasks for implementing the action:

- Develop and implement protocols for monitoring for acute deterioration in a service user's condition
- Ensure that members of the workforce are alert to signs of deterioration in a service user's mental state, including users who have not been previously identified as being at high risk.

Use care plans to manage service users at risk

Tasks for implementing the action:

- Use care plans to guide monitoring of service users who are at risk of acute deterioration in mental state; incorporate knowledge from the service user and their support people (when appropriate) about individual early warning signs
- Ensure that all members of the workforce involved in a service user's care are aware of the contents of the care plan and are alert to changes that have been identified as individual markers indicating a deterioration in the service user's mental state
- Encourage service users who are experiencing deterioration in their mental state to self-report this to the service provider
- Support people who see signs that the service user's mental state is deteriorating to communicate this to the service provider.

Develop monitoring plans

No tool equivalent to observation charts for physiological deterioration exists to provide objective criteria for tracking deterioration in a service user's mental state.

The core set of signs to be monitored may include behaviour, cognitive function, perception, and emotional state. The frequency of monitoring required may vary between individual service users, and as a service user's clinical situation, clinical risks, and goals of care change.

Tasks for implementing the action:

- Using a risk-based approach, develop plans that use the agreed parameters to manage the clinical risks and needs of each service user; include the frequency, duration and types of parameters to be monitored
- Work with service users, peer workers and clinicians to design systems for developing and documenting these plans, and to ensure that the systems align with workflow and effectively meet service users' needs
- Include monitoring plans in clinical pathways for specific service user groups who have similar clinical risks and needs, but provide prompts for the workforce to consider whether the monitoring plan meets the needs of each service user, and enable them to review and modify the monitoring plan.

Workforce training

Tasks for implementing the action:

- Develop processes to ensure that the workforce is trained and competent in monitoring and interpreting changes in mental state in the digital environment
- Provide training to the workforce to develop the necessary skills to monitor service users and implement a first response to keep the person safe until arrangements are made for more review as required
- Use an audit to evaluate whether mental state monitoring practices align with policy, and provide feedback to the workforce about their practice.

Examples of evidence

Examples of evidence may include:

Policy documents about recognising and documenting acute deterioration in mental state

Screening and assessment policies and procedures for mental health in line with the model of care

Training documents about recognising acute deterioration in mental state and how to deal with reports of deterioration from the service user or their support people

Documentation of service user involvement in developing individualised monitoring plans

Results of audits of compliance with the monitoring plan systems for mental state.

Related actions

This action relates to Action 3.11 (escalating care) and Action 3.12 (responding to acute deterioration).

Useful resources

1. National Consensus Statement: Essential elements for recognising and responding to deterioration in a person's mental state. Available at: www.safetyandquality.gov.au/publications-and-resources/resource-library/national-consensus-statement-essential-elements-recognising-and-responding-deterioration-persons-mental-state[232]
2. Emergency Triage Education Kit. Available at: www1.health.gov.au/internet/main/publishing.nsf/Content/casemix-ED-triage+Review+Fact+Sheet+Documents[233]

Escalating care

Action 3.11

The service provider has protocols that specify criteria to call for emergency assistance.

Intent of the action

Care for service users whose mental state is deteriorating is escalated safely and effectively.

Reflective questions

- What process is in place to call for emergency assistance when required?

Meeting the action

Develop an escalation protocol

Develop a clear protocol for escalating care when deterioration in a person's mental state is recognised and meets agreed criteria for escalation.

- The protocol should include:
  - designation of roles and responsibilities for members of the workforce
  - criteria to decide when emergency assistance is required
  - the emergency assistance options that may be available
  - timeframes for response
- Tailor the escalation protocol to the specific digital mental health service, taking into account the:
  - model of care of the digital mental health service and the locations of service users
  - available resources, including the clinical and peer workforce skill mix
  - capacity to engage specialist and external help
- Develop partnerships with other relevant organisations if the escalation action required is outside the scope of the service provider
- Clearly document the expected escalation protocol for digital mental health services that operate for anonymous users, including the limitations of escalation related to the anonymity of the service user
- Include electronic alerting systems within the digital mental health service, including:
  - warnings to the service user of the need for emergency action to be taken
  - flags to the workforce that agreed criteria for escalation have been met
  - warnings to other agencies of risk, and of the response required – for example, inform the service user's GP.

Communicate the escalation protocol

Provide service users and their support people (if appropriate) with information about the escalation protocols that the digital mental health service employs. These can be set out in the terms and conditions or in the product information.

Provide orientation and training to members of the workforce on the use of the escalation protocol.

Implement the escalation protocol

Tasks for implementing the action:

- Provide the workforce with mechanisms to escalate care and call for emergency assistance when acute deterioration that meets the agreed criteria is recognised, noting this escalation may be internal or external
- Provide service users with mechanisms to seek emergency assistance that is relevant to their circumstance; encourage them to use this assistance when it is required
- Develop standardised and structured communication prompts and tools for the workforce to use when escalating care
- Support escalation processes with systems that encourage appropriate documentation about the service user's mental state at the point of escalation of care
- To foster positive experiences for members of the workforce who escalate care, provide education and training for responders about expected professional behaviours, and effective teamwork and communication skills
- Provide processes for members of the workforce to routinely give feedback about their experiences of escalating care; use this information to improve escalation protocols
- Periodically review the effectiveness and experience of using the escalation protocol.

Examples of evidence

Examples of evidence may include:

Policy documents about escalating care and calling for emergency assistance that identify the criteria to trigger this response and set out the nature of the emergency assistance to be sought

Training documents about mechanisms for escalating care and calling for emergency assistance

Results of audits of compliance with the mechanisms for escalating care and calling for emergency assistance

Evidence of investigations into failures to escalate and call for emergency assistance, and associated quality improvement projects.

Related actions

This action relates to Action 3.10 (recognising acute deterioration) and Action 3.12 (responding to acute deterioration).

Useful resources

1. National Consensus Statement: Essential elements for recognising and responding to deterioration in a person's mental state. Available at: www.safetyandquality.gov.au/publications-and-resources/resource-library/national-consensus-statement-essential-elements-recognising-and-responding-deterioration-persons-mental-state[232]

Responding to acute deterioration

Action 3.12

The service provider has systems to respond to service users who show signs of acute deterioration.

Intent of the action

Systems are in place to respond to service users whose mental state is deteriorating.

Reflective questions

- What processes are in place to respond to service users who show signs of acute deterioration in their mental state?

Meeting the action

The response to a deteriorating mental state should be considered as part of the design of the model of care, and must consider whether:

- The digital mental health service will respond directly
- The response involves providing information to the service user about where to seek help in view of their deteriorating mental state
- Referral will be made to an external service or an emergency service.

Develop a response protocol

Tasks for implementing the action:

- Develop a protocol for responding when a service user's mental state is deteriorating, including when the user is anonymous
- Document the roles and responsibilities for members of the service provider workforce, along with time frames for response
- Develop partnerships with other relevant organisations if responding to acute deterioration in a service user's mental state is outside the scope of the service provider
- Ensure that the process for responding to acute deterioration aligns with the model of care.

Communicate the response protocol

Provide information to service users and their support people (if appropriate) on the protocols that the digital mental health service employs for responding to a deteriorating mental state. These can be set out in the terms and conditions or in the product information.

Provide orientation, education and training for the workforce so that they understand their individual roles, responsibilities and accountabilities in the response system.

Implement the response protocol

Tasks for implementing the action:

- Ensure that members of the workforce use the system to respond to service users who show signs of acute deterioration
- Support response processes with systems that encourage appropriate documentation about the service user's mental state at the point of responding to acute deterioration of mental state
- Provide education and training for the workforce about expected professional behaviours, and effective teamwork and communication skills, and about legislative provisions that support crisis response and emergency treatment

- Provide processes for members of the workforce to routinely give feedback about the effectiveness and their experiences of responding to a deteriorating mental state, and use this information to improve response protocols.

Examples of evidence

Examples of evidence may include:

Employment documents that describe roles and responsibilities in the event of episodes of acute deterioration

Training documents about emergency interventions in the event of acute deterioration, including specialist training for responders, such as members of medical emergency teams

Evidence of clinician competency assessment – for example, through simulation exercises, peer-review or formal assessments

Information provided to service users about options to get urgent assistance from an alternative service, for example, 000, GP, emergency department.

Related actions

This action relates to Action 3.10 (recognising acute deterioration) and Action 3.11 (escalating care).

Useful resources

1. National Consensus Statement: Essential elements for recognising and responding to deterioration in a person's mental state. Available at: www.safetyandquality.gov.au/publications-and-resources/resource-library/national-consensus-statement-essential-elements-recognising-and-responding-deterioration-persons-mental-state[232]

Glossary

If appropriate, glossary definitions from external sources have been adapted to fit the context of the National Safety and Quality Digital Mental Health Standards.

abuse: improper treatment or treatment with bad effect or for a bad purpose.

accessibility: the design of products, devices, services or environments so as to be usable by people with the widest possible range of abilities, operating within the widest possible variety of situations. For example, web accessibility means that websites, tools and technologies are designed, and developed so that people with disabilities can use them.[234]

actions for treatment: the activities or behaviours recommended to be undertaken by a service user to achieve the intended outcomes of treatment.

acute deterioration: psychological or cognitive changes that may indicate a worsening of the service user's health status; this may occur across hours or days.

alert: warning of a potential risk to a service user.

anonymity: the condition of being anonymous; an individual dealing with an entity cannot be identified and the entity does not collect personal information or identifiers.[235]

approved identifiers: items of information accepted for use in identification, including family and given names, date of birth, sex, address, healthcare record number and Individual Healthcare Identifier. Service providers and clinicians are responsible for specifying the approved items for identification and procedure matching.

assessment: a clinician's evaluation of a disease or condition based on the service user's subjective report of the symptoms and course of the illness or condition, and the clinician's objective findings. These findings include data obtained through laboratory tests, physical examination and medical history, and information reported by carers, family members and other members of the healthcare team.[236]

assistive technologies: any device, system or design that allows an individual to perform a task that they would otherwise be unable to do, or increases the ease and safety with which a task can be performed, or anything that assists individuals to carry out activities.[237]

audit: a systematic review against a predetermined set of criteria.[238]

Australian Charter of Healthcare Rights: specifies the key rights of service users when seeking or receiving healthcare services. Health ministers endorsed it in 2008.[239]

Australian Open Disclosure Framework: endorsed by health ministers in 2013, it provides a framework for health service organisations and clinicians to communicate openly with service users when health care does not go to plan.[48]

authentication: the act of proving the identity of a service user. *See also* identification

backup: a copy of digital data taken and stored elsewhere so that it may be used to restore the original after a data loss event.

barriers: something that prevents, or limits, what someone can do or find.

best practice: when the assessment, diagnosis, treatment or care provided is based on the best available evidence, which is used to achieve the best possible outcomes for service users.

best-practice guidelines: a set of recommended actions that are developed using the best available evidence. They provide clinicians with evidence-informed recommendations that support clinical practice, and guide clinician and service user decisions about appropriate healthcare in specific clinical practice settings and circumstances.[240]

business decision-making: decision-making regarding service planning and management by a service provider. It covers the procurement

of digital mental health services, purchase or contracting of equipment; program maintenance; workforce training for safe handling of services and equipment; and all issues for which business decisions are taken that might affect the safety and wellbeing of service users and the workforce.

carer: a person who provides personal care, support and assistance to another individual who needs it because they have mental health issues, problematic substance use or suicidal behaviours. An individual is not a carer merely because they are a spouse, de facto partner, parent, child, other relative or guardian of an individual, or live with an individual who requires care. A person is not considered a carer if they are paid, a volunteer for an organisation, or caring as part of a training or education program.[241]

clinical communication: the exchange of information about a person's care that occurs between treating clinicians, service users, carers and families, and other members of a multidisciplinary team. Communication can be through several different channels, including face-to-face meetings, telephone, written notes or other documentation, and electronic means. *See also* communication process

clinical governance: an integrated component of corporate governance of healthcare organisations. It ensures that everyone – from frontline clinicians to managers and members of governing bodies, such as boards – is accountable to service users and the community for assuring the delivery of safe, effective and high-quality services. Clinical governance systems provide confidence to service users and the healthcare organisation that systems are in place to deliver safe and high-quality health care.

clinician: a healthcare provider, trained as a health professional, including registered and non-registered practitioners.

communication mechanisms: channels to enable productive imparting, sharing or exchange of data or information.

communication process: the method of exchanging information about a person's care. It involves several components and includes the sender (the person who is communicating the information), the receiver (the person receiving the information), the message (the information that is communicated) and the channel of communication.

complaints management system: a staged way of receiving, recording, processing, responding to and reporting on complaints, as well as using them to improve services and decision-making.[242]

compliance: forced adherence to a law, regulation, rule, standard, process or practice.

confidentiality: the state of keeping or being kept secret or private.

conformance: voluntary adherence to a standard, rule, specification, requirement, design, process or practice.

consumer: a person who has used, or may potentially use, digital mental health services. A healthcare consumer may also act as a consumer representative to provide a consumer perspective, contribute consumer experiences, advocate for the interests of current and potential service users, and take part in decision-making processes.[243]

critical information: information that has a considerable impact on a service user's health, wellbeing or ongoing care (physical or psychological). The availability of critical information may require a clinician to reassess or change a service user's care plan.

cultural safety: identifies that health consumers are safest when clinicians have considered power relations, cultural differences and patients' rights. Part of this process requires clinicians to examine their own realities, beliefs and attitudes.

Cultural safety is defined not by the clinician but by the health consumer's experience – the individual's experience of the care they are given, and their ability to access services and to raise concerns.

The essential features of cultural safety are:

- An understanding of one's culture
- An acknowledgement of difference, and a requirement that caregivers are actively mindful and respectful of difference(s)

- Informed by the theory of power relations; any attempt to depoliticise cultural safety is to miss the point
- An appreciation of the historical context of colonisation, the practices of racism at individual and institutional levels, and their impact on First Nations people's living and wellbeing, in both the present and the past
- That its presence or absence is determined by the experience of the recipient of care and not defined by the caregiver.[23]

culture of safety: a commitment to safety that permeates all levels of an organisation, from the clinical workforce to executive management. Features commonly include acknowledgement of the high-risk, error-prone nature of an organisation's activities; a blame-free environment in which individuals are able to report errors or near misses without fear of reprimand or punishment; an expectation of collaboration across all areas and levels of an organisation to seek solutions to vulnerabilities; and a willingness of the organisation to direct resources to deal with safety concerns.[244]

cybersecurity: the practice of protecting systems, networks, and programs from digital attacks. Cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

data at rest: inactive data that is stored physically in any digital form (e.g. databases, data warehouses, spreadsheets, archives, tapes, off-site backups, mobile devices).

data in transit: data that is communicated from one device to another through networks (cellular, Wi-Fi, or other networks) or is located in random access memory (RAM).

data security: the process of protecting digital data, throughout its lifecycle, from destructive forces and the unwanted actions of unauthorised access and data corruption. Data security includes a variety of measures such as data encryption and tokenisation, and key management practices that protect data across all applications and platforms.

data sharing agreement: a formal contract that clearly documents what data are being shared and how the data can be used. This serves to protect the agency providing the data, ensures that the data will not be misused, and prevents miscommunication on the part of the provider of the data and the agency receiving the data by making certain that any questions about data use are discussed.

destruction of data: the process of destroying digital data (e.g. stored on tapes, hard disks and other forms of electronic media) so that it is completely unreadable and cannot be accessed or used for unauthorised purposes.

deterioration in mental state: a negative change in a person's mood or thinking, marked by a change in behaviour, cognitive function, perception or emotional state. Changes can be gradual or acute; they can be observed by members of the workforce, or reported by the person themselves, or their family or carers. Deterioration in a person's mental state can be related to several predisposing or precipitating factors, including mental illness, psychological or existential stress, physiological changes, cognitive impairment (including delirium), intoxication, withdrawal from substances, and responses to social context and environment.

device: a piece of equipment or a mechanism designed to serve a special purpose or perform a special function – for example, a smartphone or other electronic device.

digital health: the convergence of digital technologies with healthcare to enhance the efficiency of healthcare delivery and make medicine more personalised and precise. It may include both hardware and software solutions and services, including telemedicine, web-based analysis, email, mobile phones and applications, text messages, wearable devices, and clinic or remote monitoring sensors.

digital mental health service: a mental health, suicide prevention, or alcohol and other drug service in the form of information; digital counselling; treatment (including assessment, triage and referral); or peer-to-peer service that is delivered to a service user via a digital means.

digital literacy: the ability to identify and use technology confidently, creatively and critically to meet the demands and challenges of life, learning and work in a digital society.[245]

digital operating system: the set of programs which are used to link a computer's hardware resources with the user's software applications.[246]

dignity: the state or quality of being worthy of honour or respect.

direct care: the provision of services to a service user that require some degree of interaction between the service user and the healthcare provider.

disability: any continuing condition that restricts everyday activities. There are many different kinds of disability and they can result from accidents, illness or genetic disorders. A disability may affect mobility, ability to learn things, or ability to communicate easily, and some people may have more than one. A disability may be visible or hidden, may be permanent or temporary and may have minimal or substantial effect on a person's abilities.[247]

diversity: the varying social, economic and geographic circumstances of consumers who use, or may use, the services of a healthcare service, as well as their cultural backgrounds, disability status, religions, beliefs and practices, languages spoken, sexual orientation, gender identity and gender expression, and sex characteristics.

downloading: the process of copying data from one computer to another over a network or local connection.

effectiveness: the degree to which something is successful in producing a desired result. When something is deemed effective, it means it has an intended or expected outcome.

emergency assistance: advice or assistance provided when a service user's condition has deteriorated severely.[248]

environment: the context or surroundings in which care is delivered. For digital mental health services, technology and digital devices enable it. Environment can also include other service users and the workforce.

escalation of care: an intervention to raise concerns with a healthcare professional about the clinical deterioration of a service user. Its purpose is to summon healthcare professionals to assess and respond to the concerns. It serves as a safety mechanism so that service users who become acutely unwell may be identified early and managed in a timely manner.[249]

ethics: a set of concepts and principles that guide us in determining what behaviour helps or harms sentient creatures.[250]

evaluation: a process that critically examines a program or service. It involves collecting and analysing information about a program's or service's activities, characteristics, and outcomes. Its purpose is to make judgements about a program or service, to improve its effectiveness and to inform programming decisions.

evidence-based: any practice that relies on scientific evidence for guidance and decision-making.

evidence-informed: any practice that uses local experience and expertise with the best available evidence from research (although this may be limited) to identify the potential benefits, harms and costs of an intervention.

experience of care: the types of interactions that service users have with the digital mental health care system, including their care from their health plan, the workforce involved in delivering the service, and the service provider.

exploitation: the use of people's vulnerability, or taking unfair advantage of them for one's own benefit.

goals of care: clinical and other goals for a service user's episode of care that are determined in the context of a shared decision-making process.

governance: the set of relationships and responsibilities established by a service provider between its executive, workforce and stakeholders (including service users). Governance incorporates the processes, customs, policy directives, laws and conventions affecting the way an organisation is directed, administered or controlled. Governance arrangements provide the structure for setting the corporate objectives (social, fiscal, legal, human resources) of the organisation and the means to achieve the objectives. They also specify the mechanisms

for monitoring performance. Effective governance provides a clear statement of individual accountabilities within the organisation to help align the roles, interests and actions of different participants in the organisation to achieve the organisation's objectives. In the NSQDMH Standards, governance includes both clinical and technical governance, which are integrated components of corporate governance.

governing body: a board, chief executive officer, organisation owner, partnership or other highest level of governance (individual or group of individuals) that has ultimate responsibility for strategic and operational decisions affecting safety and quality.

guidelines: clinical practice guidelines are systematically developed statements to assist clinician and service user decisions about appropriate healthcare for specific circumstances.[251]

hardware: any physical device used in or with your digital service – for example, a computer, monitor, mouse, telephone or videoconferencing unit.

harm: an act that causes loss or pain.

health literacy: the Australian Commission on Safety and Quality in Health Care separates health literacy into two components – individual health literacy and the health literacy environment.

Individual health literacy is the skills, knowledge, motivation and capacity of a service user to find, understand, appraise and apply information to make effective decisions about health and health care, and take appropriate action.

The health literacy environment is the infrastructure, policies, processes, materials, people and relationships that make up the healthcare system, and which affect the ways in which service users find, understand, appraise and apply health-related information and services.[252]

health information: information or an opinion, that is also personal information, about the health or disability of an individual, or a health service provided or to be provided; or other personal information collected to provide or in providing a health service.[253]

healthcare record: includes a record of the service user's medical history, treatment notes, observations, correspondence, investigations, test results, photographs, prescription records and medication charts for an episode of care.

identification: the act of indicating a person's identity. *See also* authentication

incident: an event or circumstance that resulted, or could have resulted, in unintended or unnecessary harm to a service user; or a complaint, loss or damage. An incident may be clinical or technical in nature.

information and data inventory: a high-level list of the data and information that an organisation collects, where it is held, with whom it is shared, and how it is used.

information security: the practice of preventing unauthorised access, use, disclosure, disruption, modification, inspection, recording or destruction of information.

information security management system: a set of policies and procedures for systematically managing an organisation's sensitive data. It aims to protect the confidentiality, availability, and integrity of assets from threats and vulnerabilities, minimise risk and ensure business continuity by proactively limiting the impact of a security breach.

informed consent: a process of communication between a service user and service provider about options for treatment, care processes, data management or potential outcomes.[254] This communication results in the service user's authorisation or agreement to take part in planned care or data management. The communication should ensure that the service user has an understanding of the care they will receive or the data to be managed, all the available options and the expected outcomes.[255]

in-product sales: the offering of products for sale embedded within a digital mental health service.

intended user demographic: the information (e.g. age, gender) about service users for whom the service is intended.

internal access controls: security features that control how users and systems communicate and interact with other systems and resources – for example, through authentication and authorisation, regular automated monitoring and verifying of access configurations, auditing of user access to data, and control policies that make sure users are who they say they are and that they have appropriate access to data.[256]

interoperability: the ability of computerised systems to connect and communicate with one another readily to exchange and make use of data and information.

jurisdictional requirements: systematically developed statements from state and territory governments about appropriate healthcare or service delivery for specific circumstances.[251] Jurisdictional requirements encompass a number of types of documents from state and territory governments, including legislation, regulations, guidelines, policies, directives and circulars. Terms used for each document may vary by state and territory.

leadership: having a vision of what can be achieved, and then communicating this to others, and building strategies for realising the vision. Leaders motivate people and can negotiate for resources and other support to achieve goals.[257]

mental state: *See* deterioration in mental state

minimum information content: the content of information that must be contained and transferred in a particular type of clinical handover. What is included as part of the minimum information content will depend on the context and reason for the handover or communication.[258]

model of care: the way a health service is to be delivered. It outlines best-practice care and services for a person, population group or service cohort as they move through the stages of a condition. It aims to ensure service users get the right care, at the right time, by the right team and in the right place.[259]

open disclosure: an open discussion with a service user and their support people about an incident that resulted in harm to the service user while receiving care. The criteria of open disclosure are an expression of regret, and a factual explanation of what happened, the potential consequences, and the steps taken to manage the event and prevent recurrence.[260]

opt-out mechanism: a way for a service user to take action to withdraw or withhold their consent.

orientation: a formal process of informing and training a worker or contractor starting in a new position or beginning work for an organisation, which covers the policies, processes and procedures applicable to the organisation.

outcome: the status of an individual, group of people or population that is wholly or partially attributable to an action, agent or circumstance.[261]

ownership of data: the act of having legal rights and complete control over a single piece or set of data elements.

partnership: a situation that develops when service users are treated with dignity and respect, when information is shared with them, and when participation and collaboration in healthcare processes are encouraged and supported to the extent that service users choose.

patch: publicly released update to fix a known bug/issue.

person-centred care: an approach to the planning, delivery and evaluation of health care that is founded on mutually beneficial partnerships among service providers and service users.[262] Person-centred care is respectful of, and responsive to, the preferences, needs and values of service users. Key dimensions of person-centred care include respect, emotional support, physical comfort, information and communication, continuity and transition, care coordination, involvement of carers and family, and access to care.[263] Also known as patient-centred care or consumer-centred care.

peer support: a system of giving and receiving help founded on key principles of respect, shared responsibility, and mutual agreement

about what is helpful. It is about understanding another's situation empathically through the shared experience of emotional and psychological pain. When people find affiliation with others they feel are 'like' them, they feel a connection. This connection, or affiliation, is a deep, holistic understanding based on mutual experience in which people are able to 'be' with each other without the constraints of traditional (expert–patient) relationships.[264]

performance: the level of accomplishment of a given task measured against pre-set, known standards.

personal data: data about an identified individual, or an individual who is readily identifiable; for example, name, address, date of birth.

platform: a group of technologies that are used as a base upon which other applications, processes or technologies are developed. Historically, application programs written for one platform would not work on a different platform. New standards-based interfaces and open interfaces allow application programs to run on multiple platforms. Additionally, software developers have developed software tools that allow applications to run on multiple platforms.[265]

policy: a set of principles that reflect the organisation's mission and direction. All procedures and protocols are linked to a policy statement.

privacy: the right to be free from interference and intrusion, to associate freely with whom you want and to be able to control who can see or use information about you. Information privacy is about promoting the protection of information that says who we are, what we do and what we believe.[82]

privacy impact assessment: a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact.[51]

procedure: the set of instructions to make policies and protocols operational, which are specific to an organisation.

process: a series of actions or steps taken to achieve a particular goal.[266]

product information: information written by the service provider responsible for the digital mental health service that provides objective information about the quality, safety and effectiveness of the service as well as its purpose and intended users.

program: an initiative, or series of initiatives, designed to deal with a particular issue, with resources, a time frame, objectives and deliverables allocated to it.

protocol: an established set of rules used to complete tasks or a set of tasks.

pseudonym: a name, term or descriptor that is different to an individual's actual name.[235]

quality: the standard of something as measured against other things of a similar kind; the degree of excellence of something.

quality improvement: the combined efforts of the workforce and others – including service users and their support people, researchers, planners and educators – to make changes that will lead to better service user outcomes (health), better system performance (care) and better professional development.[267] Quality improvement activities may be undertaken in sequence, intermittently or continually.

Rainbow tick assessment: a quality framework comprising six standards owned and developed by Rainbow Health Australia to help health and human services organisations show that they are safe, inclusive and affirming services and employers for the LGBTIQ community. Accreditation is provided by Quality Innovation Performance and the Australian Council on Healthcare Standards.

recovery (data): a process of salvaging (or retrieving) inaccessible, lost, corrupted, damaged or formatted data from secondary storage, removable media or files, when the data stored in them cannot be accessed in a normal way.

recovery (mental health): being able to create and live a meaningful and contributing

life in a community of choice with or without the presence of mental health issues.

regularly: occurring at recurring intervals. The specific interval for regular review, evaluation, audit or monitoring needs to be determined for each case. In the NSQDMH Standards, the interval should be consistent with best practice, risk based, and determined by the subject and nature of the activity.

risk assessment: assessment, analysis and management of risks. It involves recognising which events may lead to harm in the future and minimising their likelihood and consequences.[268]

risk management: the design and implementation of a program to identify and avoid or minimise risks to service users, employees, volunteers and the organisation.

risk: the chance of something happening that will have a negative impact. Risk is measured by the consequences of an event and its likelihood.

risk-based approach: an approach that identifies, assesses, and understands the risks, and takes appropriate mitigation measures appropriate to the level of risk.

safety: the condition of being protected from harm or other non-desirable outcomes.

scope of clinical practice: the extent of an individual clinician's approved clinical practice within an organisation, based on the clinician's skills, knowledge, performance and professional suitability, and the needs and service capability of the organisation.[269]

screening: a process of identifying service users who are at risk, or already have an illness or injury. Screening requires enough knowledge to make a clinical judgement.[270]

self-harm: includes self-poisoning, overdoses and minor injury, as well as potentially dangerous and life-threatening forms of injury. Self-harm is a behaviour and not an illness. People self-harm to cope with distress or to communicate that they are distressed.[271]

service context: the particular context in which care is delivered. The service context will depend on the organisation's function, size and organisation of care regarding service delivery mode, location and workforce.[229]

service provider: an organisation that provides digital mental health services to service users, either free of charge or at a cost. A service provider may make available one or more services from which service users can select and has in place a system to oversee the delivery of the service. A developer of a digital mental health service that makes the service directly available to service users is a service provider.

service user: a person who has used, or may potentially use, a digital mental health service. A service user may be a consumer or a carer or a support person, depending on the nature of the service.

software: a collection of code instructing a computer to do specific tasks. Software includes programs, applications, scripts and sets of instructions.

standard: agreed attributes and processes designed to ensure that a product, service or method will perform consistently at a designated level.[261]

support people: individuals who provide support and reassurance to service users.

system: the resources, policies, processes and procedures that are organised, integrated, regulated and administered to accomplish a stated goal. A system:

- Brings together risk management, governance, and operational processes and procedures, including education, training and orientation
- Deploys an active implementation plan; feedback mechanisms include agreed protocols and guidelines, decision-support tools and other resource materials
- Uses several incentives and sanctions to influence behaviour and encourage compliance with policy, protocol, regulation and procedures.

technical fault: an abnormal condition or defect at the component, equipment, or subsystem level which may lead to a failure.

technical governance: the system by which the current and future use of information and communication technology is directed and controlled. It is an integrated component of the corporate governance of healthcare organisations and includes leadership, organisational structures, strategy, policies and processes to ensure that the organisation's information technology sustains and extends the organisation's strategies and objectives.

technician: a person skilled in the technique of a craft or employed to do practical work or look after software and technical equipment.

terms and conditions: the rules that apply to fulfilling a particular contract and that form an integral part of that contract. Service users and service providers must agree the terms and conditions to form a contract.

transitions of care: situations when all or part of a service user's care is transferred between services or providers, as the service user's conditions and care needs change.[272]

updates: an updated version of a digital mental health service.

usability: the extent to which a product (such as a device, service, or environment) can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use.[273]

workforce: all people working for a service provider, including clinicians, technicians and any other employed or contracted, locum, agency, student, volunteer or peer workers. The workforce can be members of the organisation or company representatives providing technical support who have assigned roles and responsibilities for care of, administration of, support of, or involvement with service users in the organisation. *See also* clinician *and* technician

References

1. Department of Health. Australian Government response to contributing lives, thriving communities – review of mental health programmes and services. Canberra: Australian Government; 2015.

2. Titov N, Dear BF, Staples LG, Bennett-Levy J, Klein B, Rapee RM, et al. The first 30 months of the MindSpot Clinic: evaluation of a national e-mental health service against project objectives. Aust N Z J Psychiatry 2017;51(12):1227–39.

3. Andrews G, Titov N. Is internet treatment for depressive and anxiety disorders ready for prime time? Med J Aust 2010;192(S11):S45–7.

4. McDermott R, Dozois DJA. A randomized controlled trial of Internet-delivered CBT and attention bias modification for early intervention of depression. J Exp Psychopathol 2019;10(2):2043808719842502.

5. Titov N, Dear BF, Nielssen O, Wootton B, Kayrouz R, Karin E, et al. User characteristics and outcomes from a national digital mental health service: an observational study of registrants of the Australian MindSpot Clinic. Lancet Digit Health 2020;2(11):e582–93.

6. Bauer M, Glenn T, Geddes J, Gitlin M, Grof P, Kessing LV, et al. Smartphones in mental health: a critical review of background issues, current status and future concerns. Int J Bipolar Disord 2020;8(1):2.

7. Baumel A, Torous J, Edan S, Kane JM. There is a non-evidence-based app for that: a systematic review and mixed methods analysis of depression- and anxiety-related apps that incorporate unrecognized techniques. J Affect Disord 2020;273:410–21.

8. Marshall JM, Dunstan DA, Bartik W. Clinical or gimmickal: the use and effectiveness of mobile mental health apps for treating anxiety and depression. Aust N Z J Psychiatry 2020;54(1):20–8.

9. Parker L, Bero L, Gillies D, Raven M, Grundy Q. The 'hot potato' of mental health app regulation: a critical case study of the Australian policy arena. Int J Health Policy Manag 2019;8(3):168–76.

10. Australian Commission on Safety and Quality in Health Care. National safety and quality digital mental health standards. Sydney: ACSQHC; 2020.

11. Australian Commission on Safety and Quality in Health Care. National safety and quality health service standards (2nd ed.). Sydney: ACSQHC; 2017.

12. Australian Commission on Safety and Quality in Health Care. Mapping of national safety and quality digital mental health standards with the national safety and quality health service standards. Sydney: ACSQHC; 2021.

13. International Standards Organization, International Electrotechnical Commission. ISO/IEC 27001: 2018: information security management [Internet]. ISO; 2018 [cited 2021 Sep 27]. Available from: https://www.iso.org/isoiec-27001-information-security.html

14. Bismark MM, Studdert DM. Governance of quality of care: a qualitative study of health service boards in Victoria, Australia. BMJ Qual Saf 2014;23(6):474–82.

15. Mannion R, Freeman T, Millar R, Davies H. Effective board governance of safe care: a (theoretically underpinned) cross-sectioned examination of the breadth and depth of relationships through national quantitative surveys and in-depth qualitative case studies. Health Serv Deliv Res 2016;4(4).

16. Taylor N, Clay-Williams R, Hogden E, Braithwaite J, Groene O. High performing hospitals: a qualitative systematic review of associated factors and practical strategies for improvement. BMC Health Serv Res 2015;15:244.

17. Australian Commission on Safety and Quality in Health Care. National model clinical governance framework. Sydney: ACSQHC; 2017.

18. Australian Health Practitioner Regulation Agency. The National Scheme's Aboriginal and Torres Strait Islander Health and Cultural Safety Strategy 2020–2025: AHPRA; 2020.

19. Australian Health Ministers' Advisory Council. A national framework for recovery-oriented mental health services: policy and theory. Canberra: AHMAC; 2013.

20. Australian Government. National Agreement on Closing the Gap: 3. Objective and outcomes [Internet]. Canberra: Australian Government; 2020 [cited 2021 Sep 27]. Available from: https://www.closingthegap.gov.au/national-agreement/national-agreement-closing-the-gap/3-objective-and-outcomes

21. Commonwealth of Australia. National Aboriginal and Torres Strait Islander Health Plan 2013–2023. Canberra: Commonwealth of Australia; 2013.

22. Australian Commission on Safety and Quality in Health Care. The national safety and quality health service standards user guide for Aboriginal and Torres Strait Islander health. Sydney: ACSQHC; 2017.

23. National Aboriginal and Torres Strait Islander Health Standing Committee of the Australian Health Ministers' Advisory Council. Cultural respect framework 2016–2026 for Aboriginal and Torres Strait Islander health. Canberra: AHMAC; 2016.

24. Embrace Multicultural Mental Health. Framework for mental health in multicultural Australia: towards culturally inclusive service delivery [Internet]. 2021 [cited 2021 Sep 27]. Available from: https://embracementalhealth.org.au/service-providers/framework-landing

25. Multicultural Mental Health Australia. National cultural competency tool (NCCT) for mental health services. Parramatta: MMHA; 2010.

26. National LGBTIQ Health Alliance. Snapshot of mental health and suicide prevention statistics for LGBTI people, February 2020. National LGBTIQ Health Alliance; 2020.

27. National Mental Health Commission. Equally well consensus statement: improving the physical health and wellbeing of people living with mental illness in Australia. Sydney: NMHC; 2016.

28. Australian Institute of Health and Welfare. Australia's welfare 2015. (Australia's welfare series No. 12. Cat. No. AUS 189). Canberra: AIHW; 2015.

29. National Rural Health Alliance. Mental health in rural and remote Australia. Canberra: NRHA; 2017.

30. Australian Institute of Health and Welfare. Health of people with disability [Internet]. Canberra: AIHW; 2020 [cited 2021 Sep 27]. Available from: https://www.aihw.gov.au/reports/australias-health/health-of-people-with-disability

31. Australian Digital Health Agency. Cyber security [Internet]. ADHA; 2021 [cited 2021 Sep 27]. Available from: https://www.digitalhealth.gov.au/healthcare-providers/cyber-security

32. Gillon R. Medical ethics: four principles plus attention to scope. BMJ 1994;309(6948):184–8.

33. Collste G. Applied and professional ethics. KEMANUSIAAN: Asian J Humanities 2012;19(1):17–33.

34. Raval V. Information ethics: information ethics in the mid-21st century. ISACA Journal 2016;6:1–6.

35. IEEE 7000-2021 Standard Model Process for Addressing Ethical Concerns During System Design. Available from: https://engagestandards.ieee.org/ieee-7000-2021-for-systems-design-ethical-concerns.html?utm_source=ieeesa&utm_medium=aem&utm_campaign=ais-2021

36. Vold K, Peters D, Calvo R, Robinson D. Responsible innovation in online therapy. Imperial Consultants, Ltd.; 2019.

37. Kerridge I, Lowe M, Stewart C. Ethics and law for the health professions (4th ed.). Annandale: Federation Press; 2013.

38. Safety and Quality Partnership Standing Committee. National practice standards for the mental health workforce 2013. Melbourne: Victorian Government Department of Health; 2013.

39. Australian Competition and Consumer Commission. Product safety [Internet]. ACCC; 2021 [cited 2021 Sep 27]. Available from: https://www.accc.gov.au/business/treating-customers-fairly/product-safety

40. Grundy Q, Parker L, Raven M, Gillies D, Mintzes B, Jureidini J, et al. Finding peace of mind: navigating the marketplace of mental health apps. Sydney: Australian Communications Consumer Action Network; 2017.

41. Royal Australian and New Zealand College of Psychiatrists. Mental health legislation and psychiatrists: putting the principles into practice [Internet]. RANZCP; 2017 [cited 2021 Sep 27]. Available from: https://www.ranzcp.org/news-policy/policy-and-advocacy/position-statements/mental-health-legislation-and-psychiatrists

42. International Standards Organization. ISO 31000, Risk management [Internet]. ISO; 2018 [cited 2021 Sep 27]. Available from: https://www.iso.org/iso-31000-risk-management.html

43. Australian Cyber Security Centre. Guidelines for system management. Canberra: Australian Signals Directorate; 2021.

44. Australian Digital Health Agency. Information security guide for small healthcare businesses. ADHA; 2018.

45. Office of the Australian Information Commissioner. Data breach action plan for health service providers [Internet]. Sydney: OAIC; 2020 [updated 2020 Feb 11; cited 2021 Sep 28]. Available from: https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-action-plan-for-health-service-providers

46. Queensland Health. Best practice guide to clinical incident management. Fortitude Valley: Queensland Government; 2014.

47. Clinical Excellence Commission. Incident management policy resources [Internet]. Sydney: CEC; 2020 [cited 2021 Sep 28]. Available from: https://www.cec.health.nsw.gov.au/Review-incidents/incident-management-policy-resources

48. Australian Commission on Safety and Quality in Health Care. Australian open disclosure framework. Sydney: ACSQHC; 2013.

49. Health Issues Centre. Toolkit for health services [Internet]. HIC; 2021 [cited 2021 Sep 28]. Available from: https://hic.org.au/toolkit-for-health-services

50. Medical Board of Australia. Good medical practice: a code of conduct for doctors in Australia. Melbourne: Australian Health Practitioner Regulation Agency; 2020.

51. Office of the Australian Information Commissioner. Guide to health privacy. Sydney: OAIC; 2019.

52. Australian Government. My Health Records Act 2012. Canberra: Australian Government; 2017.

53. Australian Commission on Safety and Quality in Health Care. e-Health safety [Internet]. Sydney: ACSQHC; 2021 [cited 2021 Sep 28]. Available from: https://www.safetyandquality.gov.au/our-work/e-health-safety

54. Department of Health. Healthcare Identifiers Service – frequently asked questions [Internet]. Canberra: Australian Government; 2018 [cited 2021 Sep 28]. Available from: https://www1.health.gov.au/internet/main/publishing.nsf/Content/pacd-ehealth-consultation-faqs

55. Australian Digital Health Agency. [Internet]. ADHA; 2021 [cited 2021 Sep 28]. Available from: https://www.digitalhealth.gov.au

56. Office of the Australian Information Commissioner. My Health Record [Internet]. OAIC [cited 2021 Sep 28]. Available from: https://www.oaic.gov.au/privacy/other-legislation/my-health-record

57. Office of the Australian Information Commissioner. Rule 42 guidance [Internet]. OAIC [cited 2021 Sep 28]. Available from: https://www.oaic.gov.au/privacy/guidance-and-advice/rule-42-guidance/

58. Australian Institute of Health and Welfare. Engaging with Indigenous Australia – exploring the conditions for effective relationships with Aboriginal and Torres Strait Islander communities. (Cat. No. IHW 106). Canberra: AIHW; 2013.

59. Australian Institute of Health and Welfare. Cultural safety in health care for Indigenous Australians: monitoring framework [Internet]. Canberra: AIHW; 2021 [cited 2021 Sep 28]. Available from: https://www.aihw.gov.au/reports/indigenous-australians/cultural-safety-health-care-framework/contents/background-material

60. Bainbridge R, McCalman J, Clifford A, Tsey K. Cultural competency in the delivery of health services for Indigenous people. (Closing the Gap Clearinghouse: Issues Paper No. 13). Canberra: AIHW; 2015.

61. ICAP Program. Improving Care for Aboriginal and Torres Strait Islander Patients Resource Kit. Melbourne: Department of Health, Victoria 2013. Available from: https://www.health.vic.gov.au/publications/improving-care-for-aboriginal-and-torres-strait-islander-patients-resource-kit

62. Australian Institute of Aboriginal and Torres Strait Islander Studies. Map of Indigenous Australia [Internet]. Canberra: AIATSIS; 1996 [cited 2021 Sep 28]. Available from: https://aiatsis.gov.au/explore/map-indigenous-australia

63. Australian Council for Safety and Quality in Health Care. Standard for credentialling and defining the scope of clinical practice. Sydney: Australian Council for Safety and Quality in Health Care; 2004.

64. Department of Health. Peer workforce role in mental health and suicide prevention [Internet]. Canberra: Australian Government; 2019 [cited 2021 Sep 28]. Available from: https://www.health.gov.au/resources/publications/primary-health-networks-phn-mental-health-care-guidance-peer-workforce-role-in-mental-health-and-suicide-prevention

65. Australian Competition and Consumer Commission. Contracts & agreements [Internet]. ACCC [cited 2021 Sep 28]. Available from: https://www.accc.gov.au/consumers/contracts-agreements

66. Richmond B. A day in the life of data. Melbourne: Consumer Policy Research Centre; 2019.

67. eSafety Commissioner. Safety by design [Internet]. Canberra: Australian Government [cited 2021 Sep 28]. Available from: https://www.esafety.gov.au/about-us/safety-by-design

68. Mental Health Coordinating Council. Trauma-informed care and practice (TICP) [Internet]. Sydney: MHCC [cited 2021 Sep 28]. Available from: https://mhcc.org.au/publication/trauma-informed-care-and-practice-ticp

69. eSafety Commissioner. The eSafety guide [Internet]. Canberra: Australian Government [cited 2021 Sep 28]. Available from: https://www.esafety.gov.au/key-issues/esafety-guide

70. Australian Human Rights Commission. National principles for child safe organisations. Sydney: AHRC; 2018.

71. Australian Federal Police. ThinkUKnow: preventing online child sexual exploitation [Internet]. Canberra: AFP [cited 2021 Sep 28]. Available from: https://www.thinkuknow.org.au

72. Office of the Australian Information Commissioner. Guide to undertaking privacy impact assessments. Sydney: OAIC; 2020.

73. Office of the Australian Information Commissioner. Privacy impact assessment tool. Sydney: OAIC; 2020.

74. Office of the Australian Information Commissioner. Privacy impact assessment eLearning course [Internet]. Sydney: OAIC; 2021 [cited 2021 Sep 28]. Available from: https://education.oaic.gov.au/elearning/pia/welcome.html

75. Office of the Australian Information Commissioner. When do agencies need to conduct a privacy impact assessment? [Internet]. Sydney: OAIC; 2020 [cited 2021 Sep 28]. Available from: https://www.oaic.gov.au/privacy/guidance-and-advice/when-do-agencies-need-to-conduct-a-privacy-impact-assessment

76. Office of the Victorian Information Commissioner. Privacy impact assessment guide [Internet]. Melbourne: OVIC [cited 2021 Sep 28]. Available from: https://ovic.vic.gov.au/privacy/privacy-impact-assessment

77. New Zealand Privacy Commissioner. Privacy impact assessment toolkit [Internet]. Wellington (NZ): New Zealand Government; 2015 [cited 2021 Sep 28]. Available from: https://www.privacy.org.nz/publications/guidance-resources/privacy-impact-assessment

78. Australian Institute of Health and Welfare. The five safes framework [Internet]. Canberra: AIHW; 2021 [cited 2021 Sep 28]. Available from: https://www.aihw.gov.au/about-our-data/data-governance/the-five-safes-framework

79. Office of the Australian Information Commissioner. Australian Privacy Principles [Internet]. Sydney: OAIC [cited 2021 Sep 28]. Available from: https://www.oaic.gov.au/privacy/australian-privacy-principles

80. Office of the Australian Information Commissioner. Guide to developing an APP privacy policy. Sydney: OAIC; 2014.

81. Office of the Australian Information Commissioner. Chapter 1: APP 1 – Open and transparent management of personal information. Sydney: OAIC; 2019.

82. Office of the Australian Information Commissioner. What is a privacy policy? [Internet]. Sydney: OAIC [cited 2021 Sep 28]. Available from: https://www.oaic.gov.au/privacy/your-privacy-rights/what-is-a-privacy-policy

83. Culnane C, Leins K. Misconceptions in privacy protection and regulation. Law in Context 2020;36(2):49.

84. Culnane C, Rubinstein BIP, Teague V. Health data in an open world. ArXiv 2017;1712.05627 [cs.CY].

85. Australian Digital Health Agency. National digital health strategy and framework for action [Internet]. ADHA; 2021 [cited 2021 Sep 28]. Available from: https://www.digitalhealth.gov.au/about-us/national-digital-health-strategy-and-framework-for-action

86. Australian Medical Association. Privacy and health record resource handbook. Canberra: AMA; 2017.

87. Australian Government. Privacy Act 1988. Canberra: Commonwealth of Australia; 1988.

88. Office of the Australian Information Commissioner. Guide to data analytics and the Australian Privacy Principles [Internet]. Sydney: OAIC; 2018 [cited 2021 Sep 28]. Available from: https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-data-analytics-and-the-australian-privacy-principles

89. O'Keefe CM, Otorepec S, Elliot M, Mackey E, O'Hara K. De-identification decision-making framework. CSIRO Reports EP173122 and EP175702. Sydney: Office of the Australian Information Commissioner; 2017.

90. Information Commissioner's Office (UK). Anonymisation: managing data protection risk code of practice. ICO; 2012.

91. Office of the Australian Information Commissioner. Data breach preparation and response [Internet]. Sydney: OAIC; 2019 [cited 2021 Sep 28]. Available from: https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response

92. Office of the Australian Information Commissioner. Chapter 5: APP 5 – Notification of the collection of personal information. In: Australian Privacy Principles guidelines. Sydney: OAIC; 2019.

93. National Health and Medical Research Council, Australian Research Council, Universities Australia. National statement on ethical conduct in human research 2007 (updated 2018). Canberra: NHMRC; 2018.

94. Office of the Australian Information Commissioner. Chapter B: Key concepts. In: Australian Privacy Principles guidelines. Sydney: OAIC; 2019.

95. National Health and Medical Research Council. Ethical considerations in quality assurance and evaluation activities. Canberra: NHMRC; 2014.

96. Office of the Australian Information Commissioner. Chapter 3: APP 3 – Collection of solicited personal information. In: Australian Privacy Principles guidelines. Sydney: OAIC; 2019.

97. Australian Competition and Consumer Commission. In-app purchases. [Internet]. Canberra [cited 2021 Dec 16]. Available from: https://www.accc.gov.au/contact-us/contact-the-accc

98. Parker MH, Wardle JL, Weir M, Stewart CL. Medical merchants: conflict of interest, office product sales and notifiable conduct. Med J Aust 2011;194(1):34–7.

99. Australian Consumer Law. [Internet]. [cited 2021 Sep 29]. Available from: https://consumer.gov.au/australian-consumer-law

100. Australian Psychological Society. APS Code of Ethics. Melbourne: APS; 2007.

101. Victorian Department of Health. National code of conduct for health care workers [Internet]. Australian Health Ministers' Advisory Council; 2015. Available from: https://www.coaghealthcouncil.gov.au/NationalCodeOfConductForHealthCareWorkers

102. Aboujaoude E, Gega L. From digital mental health interventions to digital 'addiction': where the two fields converge. Front Psychiatry 2020;10:1017.

103. Australian Cyber Security Centre. Ransomware targeting Australian aged care and healthcare sectors [Internet]. Canberra: Australian Signals Directorate; 2020 [cited 2021 Sep 29]. Available from: https://www.cyber.gov.au/acsc/view-all-content/alerts/ransomware-targeting-australian-aged-care-and-healthcare-sectors

104. International Standards Organization, International Electrotechnical Commission. ISO/IEC 27000: 2018: information technology [Internet]. ISO; 2018 [cited 2021 Sep 27]. Available from: https://www.iso.org/standard/73906.html

105. Australian Cyber Security Centre. Australia's cyber security strategy 2020 [Internet]. Canberra: Australian Signals Directorate; 2020 [cited 2021 Sep 29]. Available from: https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf

106. Australian Cyber Security Centre. Small business cyber security guide [Internet]. Canberra: Australian Signals Directorate; 2021 [cited 2021 Sep 29]. Available from: https://www.cyber.gov.au/acsc/view-all-content/publications/small-business-cyber-security-guide

107. Australian Prudential Regulation Authority. Prudential Standard CPS 234 – Information Security. Canberra: Australian Government; 2019.

108. Australian Digital Health Agency. Digital health security awareness [Internet]. ADHA; 2021 [cited 2021 Sep 29]. Available from: https://training.digitalhealth.gov.au/enrol/index.php?id=14

109. Australian Cyber Security Centre. Information security manual. Canberra: Australian Signals Directorate; 2021.

110. Australian Commission on Safety and Quality in Health Care. Fact sheet for service providers: using a risk management approach. Sydney: ACSQHC; 2020. Available from: https://www.safetyandquality.gov.au/publications-and-resources/resource-library/applying-nsqdmh-standards-using-risk-management-approach-fact-sheet

111. International Standards Organization. ISO 13131:2021: Health informatics – Telehealth services – Quality planning guidelines [internet]. ISO; 2021 [cited 2021 Dec 16]. Available from: https://www.iso.org/standard/75962.html

112. Royal Australian and New Zealand College of Psychiatrists. Professional practice guideline 19: telehealth in psychiatry. Melbourne: RANZCP; 2013.

113. Medical Board of Australia. Guidelines for technology-based patient consultations [Internet]. Australian Health Practitioner Regulation Agency; 2012 [cited 2021 Sep 29]. Available from: https://www.ahpra.gov.au/News/COVID-19/Workforce-resources/Telehealth-guidance-for-practitioners.aspx

114. Ahpra. Telehealth guidance for practitioners [Internet] [cited 2022 Jan 31]. Available from: https://www.ahpra.gov.au/news/covid-19/workforce-resources/telehealth-guidance-for-practitioners.aspx

115. Australian Cyber Security Centre. Getting your business back up and running [Internet]. Canberra: Australian Signals Directorate; 2021 [cited 2021 Sep 29]. Available from: https://www.cyber.gov.au/acsc/small-and-medium-businesses/getting-your-business-back-up-and-running

116. Australian Cyber Security Centre. Guidelines for system hardening. Canberra: Australian Signals Directorate; 2021.

117. Rapid7. Vulnerabilities, exploits and threats [Internet]. [cited 2021 Sep 29]. Available from: https://www.rapid7.com/fundamentals/vulnerabilities-exploits-threats

118. Digital NSW. Test for usability [Internet]. Sydney: New South Wales Government; 2021 [cited 2021 Sep 29]. Available from: https://www.digital.nsw.gov.au/digital-service-toolkit/design-standards/design-with-users-for-users/user-experience-design/test

119. Australian Bureau of Statistics. Disability, ageing and carers, Australia: summary of findings [Internet]. Canberra: ABS; 2019 [cited 2021 Sep 29]. Available from: https://www.abs.gov.au/statistics/health/disability/disability-ageing-and-carers-australia-summary-findings/latest-release

120. Australian Government. Disability Discrimination Act 1992. Canberra: Australian Government; 2010.

121. Australian Institute of Health and Welfare. Australia's health 2016: 3.15 Vision and hearing disorders. (Australia's Health Series No. 15. Cat. No. AUS 199). Canberra: AIHW; 2016.

122. Parliament of Australia (APH). The extent and causes of hearing impairment in Australia [Internet]. APH [cited 2021 Sep 29]. Available from: https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Community_Affairs/Completed_inquiries/2008-10/hearing_health/report/c02

123. Department of Health and Human Services Victoria. Technology and older people: findings from the VicHealth indicators survey. Melbourne: Victorian Government; 2013.

124. Deloitte Touche Tohmatsu. Digital consumer trends 2020: unlocking lockdown. Deloitte; 2020.

125. Australian Institute of Health and Welfare. Australia's health 2018. (Australia's Health Series No. 16, Cat. No. AUS 221). Canberra: AIHW; 2018.

126. Australian Bureau of Statistics. Census reveals a fast changing, culturally diverse nation. Canberra: ABS; 2017.

127. Australian Commission on Safety and Quality in Health Care. Australian Charter of Healthcare Rights (2nd ed.). Sydney: ACSQHC; 2019.

128. Australian Commission on Safety and Quality in Health Care. Supportive resources for the second edition of the Australian charter of healthcare rights [Internet]. Sydney: ACSQHC; 2019 [cited 2021 Sep 29]. Available from: https://www.safetyandquality.gov.au/consumers/working-your-healthcare-provider/australian-charter-healthcare-rights/supportive-resources-second-edition-australian-charter-healthcare-rights

129. Children's Hospitals Australasia. Charter on the Rights of Children and Young People in Healthcare Services in Australia. Canberra: CHA; 2017.

130. Queensland Health. Guide to informed decision-making in health care (2nd ed.). Brisbane: Queensland Government; 2017.

131. Custers B, Dechesne F, Pieters W, Schermer B, van der Hof S. Consent and privacy (No 2018/008 – ELAW). Leiden: Leiden University; 2019.

132. Department of Health WA. Consent to treatment policy. Perth: Western Australian Government; 2016.

133. Peisah C, Sorinmade OA, Mitchell L, Hertogh CM. Decisional capacity: toward an inclusionary approach. Int Psychogeriatr 2013;25(10):1571–9.

134. Capacity Australia [Internet]. 2017 [cited 2021 Sep 29]. Available from: https://capacityaustralia.org.au

135. Advance Care Planning Australia [Internet]. 2021 [cited 2021 Sep 29]. Available from: https://www.advancecareplanning.org.au

136. SA Health. Impaired decision-making factsheet. Adelaide: Government of South Australia; 2014.

137. United Nations. Convention on the Rights of Persons with Disabilities. New York: UN; 2006.

138. Healthcare Improvement Scotland. Participation toolkit [Internet]. NHS Scotland; 2020 [cited 2021 Sep 29]. Available from: https://www.hisengage.scot/toolkit.aspx

139. Bird S. Can children and adolescents consent to their own medical treatment? Aust Fam Physician 2005;34(1/2):73–4.

140. Kang M, Sanders J. Medico-legal issues. In: NSW Kids and Families, editor. Youth health resource kit: an essential guide for workers. Sydney: NSW Kids and Families; 2014:109–19.

141. Brophy L, McSherry B, Kokanovic R, Moeller-Saxone K, Herrman H. Guidelines for supported decision-making in mental health services. Melbourne: Healthtalk Australia; 2019.

142. Harding E, Wait S, Scrutton J. The state of play in person-centred care. London: Health Policy Partnership; 2015.

143. Clinical Excellence Commission. Partnering with patients, carers and families [Internet]. Sydney: CEC [cited 2021 Sep 29]. Available from: https://www.cec.health.nsw.gov.au/improve-quality/teamwork-culture-pcc/partnering-with-people/partnering-with-patients

144. Frampton S, Guastello S, Brady C, Hale M, Horowitz S, Bennett Smith S, et al. Patient-centered care improvement guide. Derby (CT): Planetree and Picker Institute; 2008.

145. Point of Care Foundation. PFCC: patient and family-centred care toolkit [Internet]. London: PCF [cited 2021 Sep 29]. Available from: https://www.pointofcarefoundation.org.uk/resource/patient-family-centred-care-toolkit

146. Network of Alcohol and other Drugs Agencies. Working with women engaged in alcohol and other drug treatment (2nd ed.). Sydney: NADA; 2016.

147. Agency for Healthcare Research and Quality. The SHARE approach: a model for shared decision making. Rockville (MD): AHRQ; 2016.

148. National Institute for Health and Care Excellence (NICE). Shared decision making [Internet]. London: NICE [cited 2021 Sep 29]. Available from: https://www.nice.org.uk/about/what-we-do/our-programmes/nice-guidance/nice-guidelines/shared-decision-making

149. Health Foundation. MAGIC: shared decision making [Internet]. HF; 2013 [cited 2021 Sep 29]. Available from: https://www.health.org.uk/funding-and-partnerships/programme/magic-shared-decision-making

150. Australian Commission on Safety and Quality in Health Care. National statement on health literacy. Sydney: ACSQHC; 2014.

151. Harris K, Jacobs G, Reeder J. Health systems and adult basic education: a critical partnership in supporting digital health literacy. Health Lit Res Pract 2019;3(3 Suppl):S33–6.

152. Conard S. Best practices in digital health literacy. Int J Cardiol 2019;292:277–9.

153. Robbins D, Dunn P. Digital health literacy in a person-centric world. Int J Cardiol 2019;290:154–5.

154. Smith B, Magnani JW. New technologies, new disparities: The intersection of electronic health and digital health literacy. Int J Cardiol 2019;292:280–2.

155. Clinical Excellence Commission. NSW health literacy framework. 2019–2024. Sydney: CEC; 2019.

156. Clinical Excellence Commission. Health literacy [Internet]. Sydney: CEC; 2019 [cited 2021 Sep 29]. Available from: https://www.cec.health.nsw.gov.au/improve-quality/teamwork-culture-pcc/person-centred-care/health-literacy

157. Health translations [database on the Internet]. Victorian Government. 2021 [cited 2021 Sep 29]. Available from: https://healthtranslations.vic.gov.au

158. Brega AG, Barnard J, Mabachi NM, Weiss BD, DeWalt DA, Brach C, et al. AHRQ Health literacy universal precautions toolkit (2nd ed.). Rockville (MD): Agency for Healthcare Research and Quality; 2015.

159. Centers for Disease Control and Prevention. Health literacy [Internet]. CDC [cited 2021 Sep 29]. Available from: https://www.cdc.gov/healthliteracy

160. Centers for Disease Control and Prevention. Simply put: a guide for creating easy-to-understand materials. Atlanta: CDC; 2009.

161. Centers for Disease Control and Prevention. Health literacy: find training [Internet]. CDC [cited 2021 Sep 29]. Available from: https://www.cdc.gov/healthliteracy/gettraining.html

162. Plain Language Action and Information Network. Plain language [Internet]. United States Government [cited 2021 Sep 29]. Available from: https://www.plainlanguage.gov

163. United States Department of Health and Human Services. Health literacy [Internet]. United States Government [cited 2021 Sep 29]. Available from: https://health.gov/our-work/national-health-initiatives/health-literacy

164. Centre for Culture, Ethnicity and Health. Supportive systems for health literacy. [Internet] [cited 2022 Jan 31]. Available from: https://www.ceh.org.au/resource-hub/supportive-systems-for-health-literacy

165. Health Consumers Queensland. Consumer representatives program: agency handbook. Brisbane: Queensland Government; 2009.

166. Osborne H. Can they understand? Testing patient education materials with intended readers. On Call. 2001 Nov.

167. Charnock D, Shepperd S. DISCERN instrument [Internet]. 1999 [cited 2021 Sep 29]. Available from: http://www.discern.org.uk/discern_instrument.php

168. Griffiths FE, Armoiry X, Atherton H, Bryce C, Buckle A, Cave JAK, et al. The role of digital communication in patient-clinician communication for NHS providers of specialist clinical services for young people [the Long-term conditions Young people Networked Communication (LYNC) study]: a mixed-methods study. Southampton: NIHR Journals Library; 2018.

169. Australian Commission on Safety and Quality in Health Care. Health literacy [Internet]. Sydney: ACSQHC; 2014 [cited 2021 Sep 28]. Available from: https://www.safetyandquality.gov.au/our-work/patient-and-consumer-centred-care/health-literacy

170. SA Health. Guide for engaging with consumers and the community. Adelaide: Government of South Australia; 2021.

171. Eastern Health. Cue cards in community languages [Internet]. Melbourne: Eastern Health; 2015 [cited 2021 Sep 29]. Available from: https://www.easternhealth.org.au/site/item/152-cue-cards-in-community-languages

172. Office of Disease Prevention and Health Promotion. Health literacy online [Internet]. ODPHP; 2016 [cited 2021 Sep 29]. Available from: https://health.gov/healthliteracyonline

173. Dogget J, Consumers Health Forum of Australia. 'Unique and essential': a review of the role of consumer representatives in health decision-making. Canberra: CHF; 2015.

174. Dalton J, Chambers D, Harden M, Street A, Parker G, Eastwood A. Service user engagement in health service reconfiguration: a rapid evidence synthesis. J Health Serv Res Policy 2016;21(3):195–205.

175. Murray Z. Community representation in hospital decision making: a literature review. Aust Health Rev 2015;39(3):323–8.

176. National Collaborating Centre for Methods and Tools. Partnership evaluation: partnership self-assessment tool [Internet]. Hamilton (ON): McMaster University; 2010 [cited 2021 Sep 29]. Available from: https://www.nccmt.ca/knowledge-repositories/search/10

177. Queensland Health. Health care providers' guide to engaging multicultural communities and consumers. Brisbane: Queensland Government; 2012.

178. VicHealth. How to co-design with young Victorians [Internet]. Melbourne: Victorian Government; 2019 [cited 2021 Sep 29]. Available from: https://www.vichealth.vic.gov.au/media-and-resources/publications/co-design

179. Auckland District Health Board. Health service co-design toolkit [Internet]. Auckland: ADHB; 2021 [cited 2021 Sep 29]. Available from: https://www.healthcodesign.org.nz

180. Agency for Clinical Innovation. A guide to build co-design capability. Sydney: ACI; 2019.

181. Agency for Healthcare Research and Quality. Guide for developing a community-based patient safety advisory council. Rockville (MD): AHRQ; 2008.

182. Agency for Clinical Innovation. Making change: designing change projects [Internet]. Sydney: ACI [cited 2021 Sep 30]. Available from: https://aci.health.nsw.gov.au/resources/redesign/change/making-change/designing

183. Point of Care Foundation. EBCD: Experience-based co-design toolkit [Internet]. London: PCF [cited 2021 Sep 29]. Available from: https://www.pointofcarefoundation.org.uk/resource/experience-based-co-design-ebcd-toolkit

184. Roper C, Grey F, Cadogan E. Co- production: putting principles into practice in mental health contexts. Melbourne: University of Melbourne; 2018.

185. Mars M, Morris S, Marchesiello B. Champions of inclusion: a guide to including LGBTIQ+ inclusive organisations. Sydney: National LGBTI Health Alliance; 2014.

186. National Mental Health Commission. Consumer and carer engagement: a practical guide. Sydney: NMHC; 2019.

187. Mind Australia, Helping Minds, Private Mental Health Consumer Carer Network (Australia), Mental Health Carers Arafmi Australia, Mental Health Australia. A practical guide for working with carers of people with a mental illness. Canberra: Mental Health Australia; 2016.

188. Health Issues Centre. Accredited courses [Internet]. Melbourne: HIC [cited 2021 Sep 30]. Available from: https://hic.org.au/accredited-courses

189. Consumers Health Forum of Australia. Guidelines for consumer representatives [Internet]. Canberra: CHF [cited 2021 Sep 30]. Available from: https://chf.org.au/guidelines-consumer-representatives

190. Cancer Australia. Consumer Involvement Toolkit [Internet]. Sydney: CA [cited 2021 Sep 30]. Available from: https://consumerinvolvement.canceraustralia.gov.au

191. Cancer Australia. Storytelling for health services. Sydney: CA; 2012.

192. Healthwatch Cambridgeshire. Guidance for collecting & using people's stories. Huntingdon (UK): HC; 2014.

193. Agency for Clinical Innovation. Collecting patient & carer stories: a guide for frontline health service staff who wish to understand and improve patient and carer experience. Sydney: ACI; 2014.

194. WA Health. Patient stories: a toolkit for collecting and using patient stories for service improvement in WA Health. Perth: Government of Western Australia; 2012.

195. Hanson N. UX maturity models – a collection [Internet]. 2017 [cited 2021 Sep 30]. Available from: https://nataliehanson.com/2017/02/13/ux-maturity-models

196. Department of the Premier and Cabinet. User-centred design toolkit [Internet]. Adelaide: Government of South Australia [cited 2021 Sep 30]. Available from: https://www.dpc.sa.gov.au/responsibilities/ict-digital-cyber-security/toolkits/user-centred-design-toolkit

197. W3C Web Accessibility Initiative. Web content accessibility guidelines (WCAG) overview [Internet]. 2021 [updated 2021 Apr 29; cited 2021 Sep 30]. Available from: https://www.w3.org/WAI/standards-guidelines/wcag

198. Assistive Technology Australia. Assistive technology [Internet]. ATA [cited 2021 Sep 30]. Available from: https://at-aust.org/home/assistive_technology/assistive_technology

199. Australian Human Rights Commission. A brief guide to the Disability Discrimination Act [Internet]. Sydney: AHRC [cited 2021 Sep 30]. Available from: https://humanrights.gov.au/our-work/disability-rights/brief-guide-disability-discrimination-act

200. Government of South Australia. Online accessibility toolkit [Internet]. Adelaide: Government of South Australia [cited 2021 Sep 30]. Available from: https://www.accessibility.sa.gov.au

201. Centre for Epidemiology and Evidence. Developing and using program logic: a guide. Sydney: New South Wales Government; 2017.

202. National Institute for Health and Care Excellence (NICE). Evidence standards framework for digital health technologies. London: NICE; 2019.

203. Australian Commission on Safety and Quality in Health Care. Template – product information for digital mental health services. Sydney: ACSQHC; 2020.

204. Department of Health. National Aboriginal and Torres Strait Islander suicide prevention strategy. Canberra: Australian Government; 2013.

205. Beyond Blue. Suicidal signs to look for in someone [Internet]. Melbourne: Beyond Blue [cited 2021 Sep 30]. Available from: https://www.beyondblue.org.au/the-facts/suicide-prevention/worried-about-someone-suicidal/suicidal-signs-to-look-for-in-someone

206. SuicideLine Victoria. Recognising suicide warning signs [Internet]. Melbourne: SuicideLine Victoria [cited 2021 Sep 30]. Available from: http://www.suicideline.org.au/worried-about-someone/recognising-suicide-warning-signs

207. Suicide Questions Answers Resources (SQUARE). Risk assessment questions [Internet]. Adelaide: SQUARE; 2013 [cited 2021 Sep 30]. Available from: https://www.square.org.au/risk-assessment/risk-assessment-questions

208. Lifeline. Data and statistics [Internet]. Lifeline [cited 2021 Sep 30]. Available from: https://www.lifeline.org.au/resources/data-and-statistics

209. Westers NJ, Muehlenkamp JJ, Lau M. SOARS model: risk assessment of nonsuicidal self-injury. Contemporary Pediatrics 2016;33(7):25–31.

210. Royal College of Psychiatrists. Assessment and management of risk to others. RCP; 2016.

211. Passos AdF, Stumpf BP, Rocha FL. Vitimização de doentes mentais. Archives Clin Psychiatry 2013;40(5):191–6.

212. de Mooij LD, Kikkert M, Lommerse NM, Peen J, Meijwaard SC, Theunissen J, et al. Victimisation in adults with severe mental illness: prevalence and risk factors. Br J Psychiatry 2015;207(6):515–22.

213. National Health and Medical Research Council Centre of Research Excellence in Suicide Prevention. Care after a suicide attempt. Sydney: National Mental Health Commission; 2015.

214. Royal Australian College of General Practitioners. Appendix 1: Nine steps to intervention. In: Hindmarsh E, Hegarty K, editors. Abuse and violence: working with our patients in general practice (4th ed.). Melbourne: RACGP; 2014.

215. National Health and Medical Research Council. Clinical practice guideline for the management of borderline personality disorder. Melbourne: NHMRC; 2012.

216. Australian Institute of Health and Welfare. National best practice guidelines for collecting Indigenous status in health data sets. (Cat. No: IHW 29). Canberra: AIHW; 2010.

217. Australian Bureau of Statistics. Indigenous status standard [Internet]. Canberra: ABS; 2014 [cited 2021 Sep 30]. Available from: https://www.abs.gov.au/statistics/standards/indigenous-status-standard/latest-release

218. Australian Institute of Health and Welfare. One simple question could help you close the gap. Canberra: AIHW; 2010.

219. Wu R. Turning the page on hospital communications slowly. BMJ Qual Saf 2017;26(1):4–6.

220. SA Health. Clinical Communication and Teamwork. [Internet] [cited 2022 Jan 31]. Available at: https://www.sahealth.sa.gov.au/wps/wcm/connect/Public+Content/SA+Health+Internet/Clinical+Resources/Clinical+Programs+and+Practice+Guidelines/Safety+and+Wellbeing/Communicating+for+safety/Clinical+handover+and+teamwork

221. UCLA Health. Communication Tools. [Internet] [cited 2022 Jan 31]. Available at: https://www.uclahealth.org/nursing/workfiles/CompetenciesEducation/LP-Saftey-CommunicationSkills.pdf

222. Agency for Healthcare Research and Quality. TeamSTEPPS Fundamentals Course: Module 3. Communication. [Internet] [cited 2022 Jan 31]. Available at: https://www.ahrq.gov/teamstepps/instructor/fundamentals/module3/igcommunication.html

223. Ausmed. Communication Skills: A guide to practice for healthcare professionals. [Internet] [cited 2022 Jan 31]. Available at: www.ausmed.com.au/cpd/guides/communication-skills

224. Porteous JM, Stewart-Wynne EG, Connolly M, Crommelin PF. iSoBAR – a concept and handover checklist: the National Clinical Handover Initiative. Med J Aust 2009;190(S11):S152–6.

225. Burgess A, van Diggele C, Roberts C, Mellis C. Teaching clinical handover with ISBAR. BMC Med Educ 2020;20(Suppl 2):459.

226. Institute for Healthcare Improvement. SBAR tool: situation–background–assessment–recommendation [Internet]. Massachusetts: IHI [cited 2021 Sep 30]. Available from: http://www.ihi.org/resources/Pages/Tools/sbartoolkit.aspx

227. Mater Health Service Brisbane. SHARED (situation, history, assessment, risk, expectation, documentation). Brisbane: ACSQHC; 2009.

228. Australian Commission on Safety and Quality in Health Care. Implementation toolkit for clinical handover improvement [Internet]. Sydney: ACSQHC; 2011 [cited 2021 Sep 30]. Available from: https://www.safetyandquality.gov.au/our-work/communicating-safety/clinical-handover/implementation-toolkit-clinical-handover-improvement

229. Australian Commission on Safety and Quality in Health Care. OSSIE guide to clinical handover improvement. Sydney: ACSQHC; 2010.

230. Agency for Healthcare Research and Quality. Implement teamwork and communication [Internet]. Rockville (MD): AHRQ; 2018 [cited 2021 Sep 30]. Available from: https://www.ahrq.gov/hai/cusp/modules/implement/index.html

231. Quality Improvement Clinic. Safe communication: design, implement and measure: a guide to improving transfers of care and handover. London: NHS England; 2015.

232. Australian Commission on Safety and Quality in Health Care. National consensus statement: essential elements for recognising and responding to deterioration in a person's mental state. Sydney: ACSQHC; 2017.

233. Department of Health. Emergency triage education kit [Internet]. Canberra: Australian Government; 2013 [cited 2021 Sep 30]. Available from: https://www1.health.gov.au/internet/main/publishing.nsf/Content/casemix-ED-Triage%20Review%20Fact%20Sheet%20Documents

234. W3C Web Accessibility Initiative. Introduction to web accessibility [Internet]. 2019 [updated 2019 June 5; cited 2020 Feb 6]. Available from: https://www.w3.org/WAI/fundamentals/accessibility-intro

235. Office of the Australian Information Commissioner. Chapter 2: APP 2 – Anonymity and pseudonymity. In: Australian Privacy Principles guidelines. Sydney: OAIC; 2019.

236. Australian Commission on Safety and Quality in Health Care. A better way to care: safe and high-quality care for service users with cognitive impairment (dementia and delirium) in hospital. Sydney: ACSQHC; 2014.

237. Independent Living Centres Australia. What is assistive technology? [Internet]. ILCA; 2011 [cited 2020 Feb 6]. Available from: https://ilcaustralia.org.au/Using_Assistive_Technology

238. Australian Commission on Safety and Quality in Health Care. Safety and quality improvement guide standard 6: clinical handover. Sydney: ACSQHC. Available from: http://www.safetyandquality.gov.au/wp-content/uploads/2012/10/Standard6_Oct_2012_WEB.pdf.

239. Australian Commission on Safety and Quality in Health Care. Australian Charter of Healthcare Rights. Sydney: ACSQHC; 2008.

240. Australian Nursing and Midwifery Federation (SA Branch). Best practice guidelines. Adelaide: ANMF; 2016.

241. Australian Government. Carer Recognition Act 2010. Canberra: Australian Government; 2010.

242. Ombudsman for the Northern Territory. Effective complaints management 1: setting the scene. Darwin: Ombudsman for the Northern Territory; 2006.

243. Consumers Health Forum of Australia. About consumer representation. Canberra: CHF; 2016.

244. Institute for Healthcare Improvement. Quality improvement and patient safety glossary. Cambridge (MA): IHI; 2015.

245. Coldwell-Neilson J. What is digital literacy? [Internet]. Decoding Digital Literacy; 2019 [cited 2020 Feb 6]. Available from: https://developingemployability.edu.au/what-is-digital-literacy

246. AT Internet. Glossary: OS (operating system) [Internet]. AT Internet [cited 2020 Feb 6]. Available from: https://www.atinternet.com/en/glossary/os-operating-system

247. Australian Network on Disability. What is disability? [Internet]. AND [cited 2020 Feb 6]. Available from: https://www.and.org.au/resources/disability-statistics/what-is-disability

248. Australian Commission on Safety and Quality in Health Care. National consensus statement: essential elements for recognising and responding to acute physiological deterioration (2nd ed.). Sydney: ACSQHC; 2017.

249. McKinney A, Fitzsimons D, Blackwood B, McGaughey J. Patient and family-initiated escalation of care: a qualitative systematic review protocol. Systematic Reviews 2019;8(1):91.

250. Elder L, Paul R. The miniature guide to understanding the foundations of ethical reasoning: Foundation for the Art of Critical Thinking; 2003.

251. Field M, Lohr K, editors. Guidelines for clinical practice: from development to use. Washington DC: National Academy Press; 1992.

252. Australian Commission on Safety and Quality in Health Care. Health literacy: taking action to improve safety and quality. Sydney ACSQHC; 2014.

253. Office of the Australian Information Commissioner. What is health information? [Internet]. OAIC [cited 2020 Feb 6]. Available from: https://www.oaic.gov.au/privacy/health-information/what-is-health-information

254. American Medical Association. Opinions on consent, communication & decision making: informed consent. Chicago (IL): AMA; 2016.

255. Carey-Hazell K. Improving patient information and decision making. Aust Health Consumer 2005;1:21–2.

256. Citrix. What is access control? [Internet]. Citrix [cited 2021 Sep30]. Available from: https://www.citrix.com/en-au/glossary/what-is-access-control.html

257. World Health Organization. Leadership and management. In: Operations manual for delivery of HIV prevention, care and treatment at primary health centres in high-prevalence, resource-constrained settings. Geneva: WHO; 2008:264–81.

258. Australian Commission on Safety and Quality in Health Care. Implementation toolkit for clinical handover improvement. Sydney: ACSQHC; 2011.

259. Agency for Clinical Innovation. Understanding the process to develop a model of care: an ACI framework. Sydney: ACI; 2013.

260. Australian Commission on Safety and Quality in Health Care. Open disclosure standard. Sydney ACSQHC; 2008.

261. Runciman WB. Shared meanings: preferred terms and definitions for safety and quality concepts. Med J Aust 2006;184(S10):S41–3.

262. Institute for Patient and Family-Centered Care (PFCC). Patient- and family-centered care [Internet]. McLean (VA): PFCC [cited 2021 Feb 6]. Available from: https://www.ipfcc.org/about/pfcc.html

263. Australian Commission on Safety and Quality in Health Care. Patient-centred care: improving quality and safety through partnerships with patients and consumers. Sydney: ACSQHC; 2011.

264. Mead S, Hilton D, Curtis L. Peer support: a theoretical perspective. Psychiatr Rehabil J 2001;25(2):131–41.

265. Technopedia. Platform [Internet]. [cited 2020 Feb 6]. Available from: https://www.techopedia.com/definition/3411/platform

266. Oxford University Press. Process. English Oxford living dictionaries. Oxford: Oxford University Press; 2015.

267. Batalden P, Davidoff F. What is 'quality improvement' and how can it transform healthcare? Qual Saf Health Care 2007;16(1):2–3.

268. National Service User Safety Agency (UK). Healthcare risk assessment made easy. London: National Health Service; 2007.

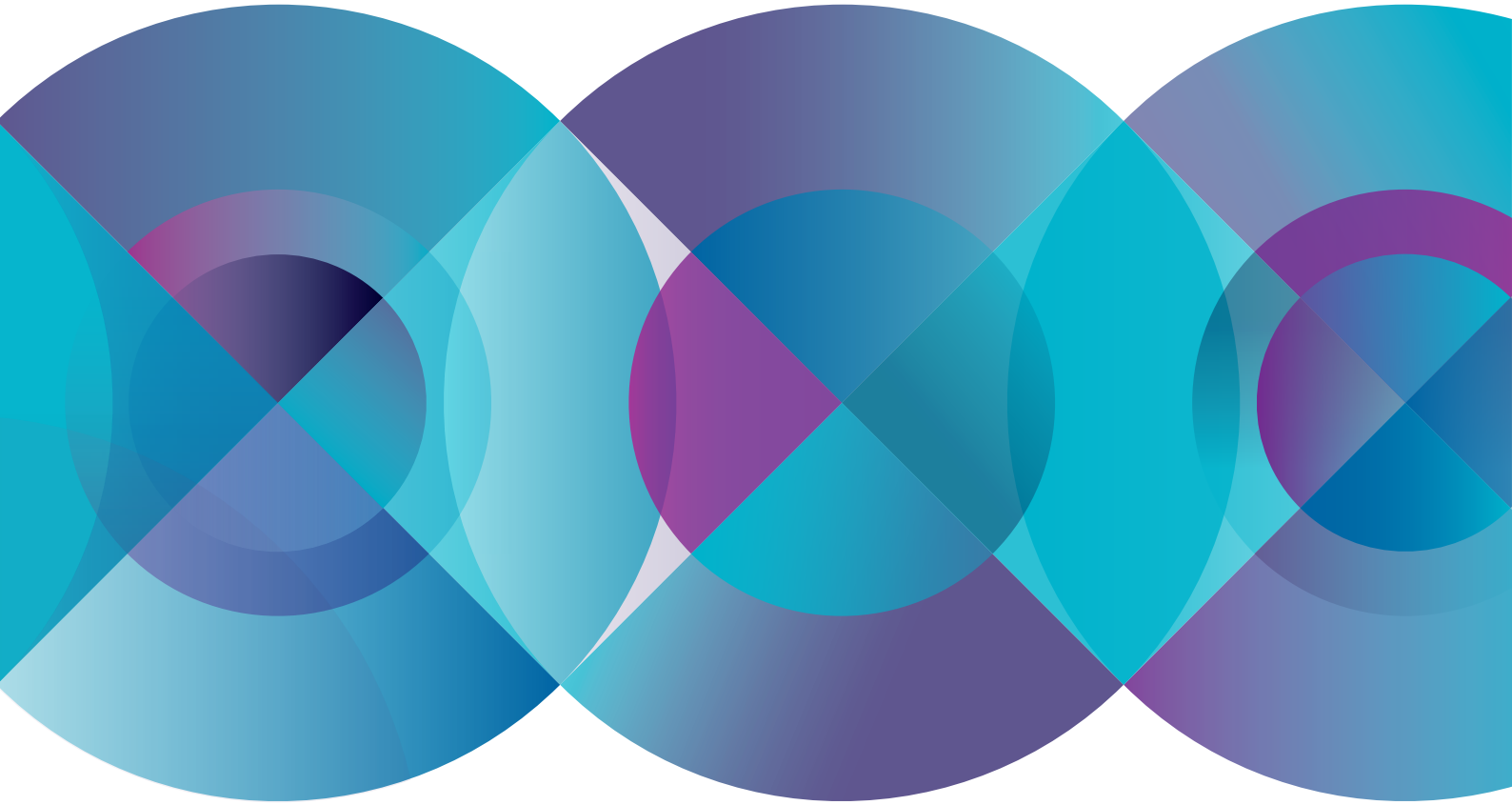
269. Australian Commission on Safety and Quality in Health Care. Safety and quality improvement guide standard 1: governance for safety and quality in health service organisations. Sydney: ACSQHC; 2012.

270. Australian Wound Management Association. Pan Pacific clinical practice guideline for the prevention and management of pressure injury. Osborne Park, WA: Cambridge Media; 2012.

271. Royal Australian and New Zealand College of Psychiatrists. Self-harm: Australian treatment guide for consumers and carers. Melbourne: RANZCP; 2009.

272. National Transitions of Care Coalition. Transitions of care measures: paper by the NTOCC Measures Work Group. Washington DC: NTOCC; 2008.

273. W3C Web Accessibility Initiative. Accessibility, usability, and inclusion [Internet]. 2016 [updated 2016 May 6; cited 2020 Feb 6]. Available from: https://www.w3.org/WAI/fundamentals/accessibility-usability-inclusion



AUSTRALIAN COMMISSION
ON SAFETY AND QUALITY IN HEALTH CARE

Level 5, 255 Elizabeth Street, Sydney NSW 2000

GPO Box 5480, Sydney NSW 2001

Phone: (02) 9126 3600

@ACSQHC

www.safetyandquality.gov.au