



A practice approach to safe and effective care

Your organisation likely delivers services using a practice approach informed by trauma-informed recovery principles. This should apply and be modified to each mode of digital service delivery as necessary. The practice approach must be relevant to the purpose and aim of the digital service, how it operates, how it applies to in-person services, and how it is informed by evidence and best practice. This information can assist consumers, and where applicable, their carers and support people, to make informed choices about digital services.

A trauma-informed recovery approach must be applied to all information provided online, including booking systems and consumer education. This will ensure that every step of a consumer's experience with your service is safe and effective, and that people are not deterred from accessing your service because they are unable to negotiate for example, your appointment booking process.

Your organisation should implement and maintain systems for the delivery of safe and high-quality care to minimise the risk of harm to service users, their support people, and others.

Checklist: A practice approach to safe and effective care

Does your organisation:

Monitor service delivery to ensure it is consistent with your recovery practice approach to care?

Assign responsibility to a particular manager or staff member for the overall accountability of the care of each consumer using the service?

Develop care plans with the consumer that include a digital service?

Deliver digital services in a way that ensures continuity of care? For example, are there alternative arrangements in place in case of any service disruptions?

Integrate digital services with the consumer's other service providers as much as possible?

Encourage the sharing of knowledge and experience with other digital service providers through e.g., communities of practice?

Refer to follow-up services and supports that are consistent with the practice approach?

Minimising harm and deterioration

In the absence of in-person interactions, minimising the risk of a consumer's mental health deteriorating in digital service delivery is critical. Without the usual environmental cues and other indicators that might suggest risk, it is necessary to screen for harm to the consumer and others. Risks include exploitation and abuse, neglect, self-harm and suicidality and risk to dependents. Early recognition of deterioration in a consumer's physical or mental health will assist in achieving best outcomes.

Where risk of deterioration is assessed, an effective response should be available, whether that is provided directly by your organisation or through referral to another organisation. It is important to effective planning of digital service delivery for staff to know the consumer's location and nearest crisis response teams, in the event additional assistance is required.

Checklist: Minimising harm and deterioration

In your organisation:

Are there assessment tools to help recognise deterioration in a consumer's mental state during digital service delivery?

Do you have a planning process that has been discussed with consumers that determines what steps should be taken if they become unwell during a digital service?

Are there protocols to respond to deterioration?

Have staff received training to respond to deterioration when delivering digital services?

Are staff trained to implement de-escalation strategies when delivering digital services?

Are there protocols for responding to consumers who present a risk of harm to self and others?

If a consumer requires healthcare needs beyond the scope of the service, are there protocols for providing appropriate information and referrals?

Are there have protocols in place for escalating care, i.e., criteria to call for emergency assistance and notifying a consumer's support network?

Communicating for safety

Communication is a key safety and quality issue. When a service user is not physically present or when they may even be accessing the service anonymously, it is critical to ensure that they are correctly identified to receive continuity of care, and that no other individual is able to inappropriately access their personal information.

Effective communication and documentation are critical when a consumer engages with a service, especially when their needs change, and when their care is transferred. Systems and processes should be in place to ensure effective communication at these times.

Checklist: Communicating for safety

Does your service:

Use appropriate identifiers for service users according to digital services best-practice guidelines?

Is the anonymity of the service users protected where this is part of the practice approach?

Communicate critical information effectively, including alerts and risks that might form part of a consumer's care?

Are there systems to document information contemporaneously regarding critical information and alerts, reassessment processes and outcomes, and changes to the care plan?

Domestic and family violence

Some perpetrators of domestic violence use phones, hidden cameras, or apps to track their victims. They may use technology to find out where their victims are, what they are doing or follow them without the victim's consent. For example, some perpetrators may download spyware on to a victim's phone access their messages and listen to their voice and video calls without the victim's knowledge.

In these situations, digital service delivery may increase risk of harm to the victim. For example, if the victim is disclosing confidential information or trying to make a safety plan to leave a relationship, the perpetrator may overhear this information. If consumers have video meetings with support workers and the chat messages are saved on the consumer's computer or in the cloud, this can compromise security if either their computer or cloud account are being tracked by the perpetrator.

Victims are not necessarily safer if they simply stop using technology. For some perpetrators, this may escalate their dangerous behaviour if they feel the victim preventing access to them and the perpetrator's control is therefore threatened. If victims stop using their phone or social media accounts altogether, they can also become more isolated from friends and family, making harder for them to get help. Some victims choose to use a safer computer, device or phone, but not disable the monitored device. This approach allows them to continue collecting evidence and minimise the risk of the perpetrator's violence escalating.

Checklist: Domestic and family violence

In your service:

Are staff trained to identify domestic and family violence, and technology-facilitated abuse in particular?

Are staff trained in the best practices in communicating with victims using the phone, video and online chat?

Are staff trained to provide basic online privacy and safety tips?

Are staff trained to create a flexible safety plan for victims experiencing technology facilitated abuse? For example, do workers ask victims if it is safe to call them and make alternative arrangements if the victim says no?

Do you have adequate record-keeping so that new workers will not accidentally contact victims in a manner that has previously been identified as unsafe?

Do intake processes risk compromising the safety of a victim experiencing technology-facilitated abuse?

Do staff refer victims to appropriate specialist domestic violence support services?

If your organisation's website provides information specifically to domestic violence victims, is there a 'quick exit' safety button?

Further resources

- [National Network to End Domestic Violence Digital Services Toolkit](#): This toolkit helps services consider how to choose appropriate digital services technology and best practices.
- [Technology Safety Plan: A Guide for Survivors and Frontline Workers](#): general information about safety planning with victims of domestic and sexual violence, stalking, and trafficking in situations of technology abuse
- [Assessing for Technology Abuse and Privacy Concerns](#): This factsheet helps frontline workers identify technology misuse by the abuser to create a safety plan
- [eSafety Commissioner Technology-facilitated abuse webpage](#): resources and information to help people deal with technology-facilitated abuse.
- [Women's Domestic Violence Court Advocacy Services](#): WDVCSs provide information, advocacy and referrals to assist women and their children who are or have been experiencing domestic and family violence, with their legal, social and welfare needs.
- [1800RESPECT](#): free, confidential national sexual assault, domestic family violence and counselling service available 24/7.

Cultural safety

Culturally safe services recognise that a consumer-centred experience involves consideration of identity and shared respect, meaning, knowledge and experience. Digital services can facilitate more culturally safe services by extending the reach of services to remote or isolated communities. For example, research at an Aboriginal Community Controlled Health Service found that telehealth could facilitate more culturally appropriate healthcare. Indigenous health workers could be present more often during telehealth consultations, because of the reduced need to travel, and provide effective advocacy and support¹.

Checklist: Cultural safety

In your service:

Have you consulted with community advisors as to what constitutes cultural safety?

Is your digital service culturally safe for consumers of different backgrounds?

¹ Caffery LJ, Bradford NK, Smith AC, Langbecker D 2018, *How telehealth facilitates the provision of culturally appropriate healthcare for Indigenous Australians*, J Telemed Telecare. 2018 Dec;24(10):676-682. doi: 10.1177/1357633X18795764. PMID: 30343658.

Feedback and complaints processes

Feedback from users of your services should be used to inform quality improvement activities and improve the safety of your organisation's digital services. In addition to consumer involvement during co-design, co-production, implementation and outcome evaluation, consumers should be part of quality assurance and continuous improvement processes.

Consumers should be able to provide feedback on their experiences of any issue relating to digital services, including the particular platform used, and the information they were provided about the service in order to participate.

Checklist: Feedback and complaints processes

Does your organisation:

Regularly seek feedback from consumers and their supporters about their experiences of the service and outcomes of care?

Use this information to improve safety, quality, performance and effectiveness?

Does your organisation's complaints management system:

Encourage and assist service users and their supporters to report complaints?

Involve service users and their supporters in the review of complaints?

Resolve complaints in a timely way?

Provide timely feedback to the service users and their supporters, the governing body, and relevant staff, on the analysis of complaints and actions taken?

Use information from the analysis of complaints to inform safety and quality improvements?

Record the risks identified from the analysis of complaints in the organisation's risk management system?

Regularly review and act to improve the effectiveness of the complaints management system?