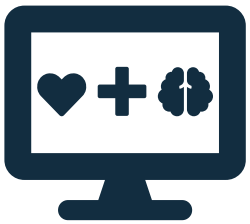

TELEHEALTH & RESPONDING TO SEXUAL VIOLENCE

TELEHEALTH OVERVIEW

Telehealth care is the delivery of health-related services and information via electronic information and telecommunication technologies compared to traditional face-to-face in-person health care.[1]

When rural settings, transportation limitations, a lack of mobility, decreased funding, a lack of staff, or stay-at-home orders restrict access to care, telehealth may bridge the gap. In the area of sexual violence response, telehealth care has been used to reach survivors in remote areas, provide ongoing support services when survivors are outside of the community, and provide anonymous help through crisis lines and hotlines.

In changing times and when technological advances have connected so many remote parts of the world, telehealth care is part of the new visioning for the future of health care.

Telehealth care is a large umbrella term that includes various tools and strategies for providing care and support to persons with the use of technology and resource sharing. It includes:

- Telemedicine (diagnosis and treatment of illness or injury)
- Services such as assessment
- Monitoring
- Communications
- Prevention
- Education

For the areas of sexual violence prevention and response, use of technology and remote learning/connection strategies have been in place for a while. Agencies have best practices and protocols in place to insure confidentiality, proper care for records and information, and proper training and supervision of employees through written, in-person, and phone communication. Lessons from the field, especially rural areas who have been using a variety of telehealth care for some time, are critical to appropriate and thoughtful use of telehealth care strategies. The following are an outline of best practice considerations when utilizing telehealth care in agencies that respond to and prevent sexual violence.

Forms of telehealth care reviewed here include phone calls, video conference calls and face-to-face video calls, email, online chat and messaging, sharing files, and social media. This is not an exhaustive list of telehealth platforms but includes the major categories that sexual violence response and prevention agencies use.

This memorandum will provide an overview of general best practices in thoughtful provision of telehealth care, as well as specific considerations for some forms of telehealth care.

1 See https://www.cdc.gov/phlp/publications/topic/telehealth.html

GENERAL BEST PRACTICES

Set Expectations

Have detailed conversations and written reference information about the forms of telehealth care the agency provides, confidentiality within those formats, and the limits of confidentiality in the agency.

- Check to make sure that there is an expectation of privacy when engaging with telehealth care. This includes not having multiple people able to see the conversation at the same time, closed door, advocate can protect privileged communication etc.
- Let survivors/clients know about the technology.
- Inform clients/survivors of their rights upfront and any limitations in confidentiality, such as mandatory reporting requirements.

Quality Services

- Advocates, volunteers, and employees should be trained on the distinct opportunities and challenges of each form of telehealth care provided at the agency.
- Have a protocol and plan for responding to inappropriate telehealth care uses. Adapt a protocol based on your organization's plan around inappropriate hotline callers or situations where counseling needs to be ended.

Decide the Level of Services

- Make sure the organization knows what forms of communication are appropriate in different situations. For instance, providing general prevention messages and information would be appropriate via social media, but personal support would not appropriate through social media public pages.
- Decide how prepared the organization is for using digital resources for the delivery of services. Review the National Network to End Domestic Violence's Technology Safety digital readiness assessment for more information.[2]

Data Security

- Gather only the information necessary for providing services. Do not record personal conversations as a general rule. Recording should be limited to creating training materials or online resources.
- Make sure the information/data is secure. Computers/servers should be under password protection and lock and key. Passwords should be difficult to guess and changed on a regular basis. Virus protection and monitoring should be part of the agency's security team/committee duties.
    - Make sure passwords are not written on materials posted on the computer.
- Know the level of encryption/types of protection for the various platforms used in telehealth.
- Review the levels of data security and update them on a continual basis.

Advocate Information and Devices

- Only gather the information needed from the advocate. For instance, do not gather IP addresses or other location information if it is not needed.
- Make sure that there is protection between personal and professional devices. If employees are allowed to use their personal devices for providing telehealth, the agency should have a protocol for protecting confidential information on those devices, which can be extremely challenging.
    - Use of personal devices can complicate and undermine the protection of confidential information.

2 https://www.techsafety.org/assessing-readiness-for-digital-services

CONSIDERATIONS FOR VARIOUS FORMS OF TELEHEALTH CARE

Phone calls (voice only or TTY)

Perhaps one of the oldest and most familiar forms of telehealth care, phone calls should not be recorded and advocates should be properly trained on providing confidential services and support via phone calls.

- Do not collect more information than needed.
- Check data security and monitoring on the telephone lines, including billing and call records.

Video conference calls, face-to-face video calls

Conference call systems such as Zoom, Google Hangouts, Skype, provide video real-time conversations. While providing human face-to-face interaction, it also opens up more situations where information can be inadvertently revealed.

- Make sure that conversations are not recorded.
- Explain the technology to the client/survivor. Do not assume that all persons using the technology have the same comfort level nor the same devices to access technology. Make sure the technology is assessible across platforms (Apple, Android, PC etc.).
- Train staff on trauma-informed video conference support.
- Make sure an expectation of privacy is set (no interruptions or unnecessary people present).
- Review the encryption and security provisions of the platform regularly.

Email

Email correspondence can be a form of communication, however it creates several ways of duplicating conversations and may not be the best method for protecting confidential communications.

- Make sure the email address signature states the protected nature of communications.
- Regularly clear/delete history, trash, inbox, and sent email boxes.
- **Even heightened encryption and clearing protocols may not sufficiently protect confidential communications if they have been seen by third parties.

Online chat, messaging, and texting:[3]

Online chat, message applications, and phone text messages are a growing area of exploration for the provision of telehealth. However, there are many considerations about the impact on confidential information that these platforms provide. Agencies should have a protocol on what formats and platforms are appropriate for what communications.

- Research and decide what forms of chat, messaging, and texting are appropriate for what level of service. Consider a spectrum of services: crisis support to counseling to prevention education to general information. As an organization, determine what levels are appropriate for chat-based services/communications. Take the National Network to End Domestic Violence's Technology Safety program digital readiness assessment for more information.[4]
- Know about the encryption and protection levels of the chat, texting and messaging services.
- Only gather information that is necessary for the provision of services. For example, online chat in a browser will often default to gathering location and IP addresses which may not be needed. This is because online browser chats were originally developed as a customer service tool that would gather a lot of information and be heavily monitored.
- Make sure advocates know how to use the online chat and messaging platforms in a confidential manner.

3 More detail in Memorandum on Online Chat and Text Services for Survivors (CALCASA 2020).
4 https://www.techsafety.org/assessing-readiness-for-digital-services

Shared files, cloud-based files/folders

More and more organizations are developing work-at-home capabilities and ways to remotely share information. With file sharing and cloud-based file storage, many organizations can now support employees working from home or remotely. These more open sources of data require thoughtful development of confidentiality and data security measures. Organizations using file sharing/cloud-based files have to take special precautions and understand the need to protect confidential information.

- Use encryption, password protection, and data security tools.
- Limit or "time-out" access to confidential information. (After a period of lack of use, have the user have to login for access).
- Do not allow sensitive information to be downloaded to personal devices.
- Provide employee training on proper use of shared files and protection of confidential information.
- Make sure access to shared files is limited to individuals who should have access. Change passwords frequently or require a two-step authentication to better verify that the appropriate person is accessing the shared information.
- Change passwords to shared files/cloud-based access after staff transitions/turnover.

Social media:

Nearly all organizations and agencies have a social media presence, website, or other ways to engage through technology with all areas community. These formats are helpful for community prevention and education that is part of telehealth care.

- Have a plan and protocol for responding to disclosures via social media.
- Make sure social medial channels are monitored for abuse and violence. Have an agency stance on what is allowed to stay on social media platforms, and what is reported or removed.
- Make sure social media platforms are password protected with frequent password changes. It is especially important after staff transitions to change passwords to social media sites.

As stated earlier, this is not an exhaustive list of the forms of technology in telehealth care. This list continues to grow as new forms of communication are invented and extended throughout the world. The amazing opportunity of telehealth care is to provide easy access to information and expand support for survivors, while continuing to safeguard confidential information.

RESOURCES

National Resources

Center for Disease Control and Prevention (CDC) Articles on Telehealth Care:

- https://www.cdc.gov/phlp/publications/topic/telehealth.html
- https://www.cdc.gov/phlp/publications/topic/anthologies/anthologies-telehealth.html

National Consortium of Telehealth Resource Centers:

- https://www.telehealthresourcecenter.org/

Serving Survivors in Rural Areas, Article:

- https://ohiovalleyresource.org/2019/03/01/serving-survivors-in-rural-states-telemedicine-brings-treatment-for-sexual-abuse/

Telehealth Care and SAMHSA (Substance Abuse and Mental Health Services Administration):

- https://store.samhsa.gov/product/In-Brief-Rural-Behavioral-Health-Telehealth-Challenges-and-Opportunities/SMA16-4989
- https://www.samhsa.gov/section-223/care-coordination/telehealth-telemedicine

Technology Safety (Project of the National Network to End Domestic Violence)

- www.techsafety.org
- https://www.techsafety.org/digital-services-during-public-health-crises

Technology Safety Assessment for Readiness for Digital Services:

- https://www.techsafety.org/assessing-readiness-for-digital-services

Using Telemedicine to Improve the Care Delivered to Sexually Abused Children in Rural, Underserved Hospitals

- https://pediatrics.aappublications.org/content/123/1/223

Other State Resources

Colorado Coalition Against Sexual Violence Digital Resource:

- https://www.ccasa.org/resources/telehealth-counseling-digital-response-resources/

Pennsylvania Coalition Against Rape Telecounseling Resource:

- https://pcar.org/resource/telecounseling-survivors

Texas Telehealth Care for Sexual Violence Survivors:

- https://mhealthintelligence.com/news/texas-launches-telehealth-program-to-help-sexual-assault-victims