This document outlines considerations for CVSSD grantees that host remote multidisciplinary team (MDT) meetings.

- Meetings must meet VOCA confidentiality requirements (and HIPAA too if medical information is shared) regardless of how the team meets.
- Signed confidentiality agreements should be collected from all members prior to the MDT meeting (just as is required for in person meetings).
- MDT members should adopt practices to ensure confidentiality at each member's remote location. The Victim Rights Law Center's "Protecting Survivor Privacy When Working from Home: A Guide for OVW-Funded Victim Services Providers" may be helpful in thinking about user-end privacy.
- Select a platform for specific type(s) of communication (video, chat, etc.) that is end-to-end encrypted (so no one can spy on or collect the information shared during the meeting) and not stored or collected by the platform vendor. Keep in mind that this may require having a Business Associate Agreement with the vendor and/or purchasing an upgraded version of a platform. **Remember** to consider all meeting platform options. A teleconference may be sufficient to meet your needs.

Consider the following questions (courtesy of the NNEDV and Techsafety):

Is this Platform Secure?

All technology is vulnerable to being hacked. It is important to thoroughly understand the security of the technology that you're using or considering. For example, if you are considering using a forum to create an online support group for survivors, is the host website secure? How easy would it be for someone to gain access to the forum to see the conversations? If you are using a private site where users must log into to be part of the conversation, are there security protocols in case the user forgets to log off and someone else (not the user) has access to the private site? While security cannot be 100% foolproof, you can take measures to ensure that the site or system you are using is as secure as it can be.

Can Other People Access or See the Data?

Services that are offered through a third party could allow others outside of your agency access to the information shared on or through the service. Even if you're using a conference call service for a support group, it could be possible that an operator or someone who works for the conference call service has the capability to enter the call, even if it's just for maintenance or quality purposes. If the technology you are using is hosted and offered through a third party, know how and what their staff has access to.

Some third party services may not allow access to the information shared or communicated through the technology but they may use aggregate data (number of callers, phone numbers, IP addresses, etc.) and share it with their other clients, advertisers, or partners to promote their services. When selecting a service, know exactly what information they will collect and for what purpose.

Does the Technology Keep a Record?

Some services may store a record of all conversations unless it's deleted by the users. Because of this, if you are offering counseling or a survivor is sharing intimate details with you, that information may be stored on the service for as long as their data retention policy dictates. Some video conferencing or phone conferences services may allow for either party to record the conversation. Be sure you know if the service you have selected allows record keeping of any kind.

Also keep in mind that since you are using a third party, if these records are kept and stored by the service provider, they may release them to law enforcement or to an attorney through a court order or subpoena. Be sure you know how this company will respond to legal requests for information, and whether it is safe for you and the survivor to share certain information through these services.

Resources including a checklist for selecting a digital services vendor can be found here.