DEPARTMENT OF JUSTICE
Elder Justice
INITIATIVE

Hosting a Virtual Elder Abuse MDT

Videoconferencing Confidentiality and Security Tips for Hosting Virtual MDT Meetings

Confidentiality and security are top concerns for teams moving to a video conferencing meeting format. Here are some tips to consider when developing your meeting protocol.

Confidentiality

- Most video conferencing platforms have HIPAA compliant for-pay tiers.
- Comply with the platform's security protocol. There are often steps you will need to take when setting up a meeting to ensure that your meetings are secure and confidentiality is preserved.
- Consider adding language to your team's confidentiality agreements to cover remote communication. If you do this, collaborate on changes with your partner agencies and any legal counsel you routinely use when developing your meeting policies and protocols.

Licensed material is being used for illustrative purposes only. Any person depicted in the licensed material is a model.

Enhancing Security

- Use 'waiting rooms' to accept participants into meetings.
- Display confidentiality agreement language in the waiting room or prior to the meeting.
- Formalize a way to confirm that participants have read, understood and agreed to confidentiality statement – email, group chat acknowledgement, sign and scan digital documents, etc.
- Expel participants for non-compliance.
- Do not use open Wi-Fi. Make sure your Wi-Fi is password protected.
- Do not hold calls in public spaces where information can be overheard or seen by others.
- Keep your software updated as companies are continually adding security updates and patches.
- Stay current with organizational protocols and professional guidelines regarding confidentiality and information sharing.