



Telepsychiatry Services Technical Guidelines Checklist for Local Providers

14 NYCRR Section 599.17(3) provides that OMH approval of telepsychiatry services in OMH licensed outpatient clinics will be based upon approval of a written plan that meets a variety of standards. Included in these standards is the following: “(i) All telepsychiatry services must be performed on dedicated service transmission linkages that meet minimum Federal and State requirements, including but not limited to 45 CFR Parts 160 and 164 (HIPAA Security Rules) and which are consistent with guidelines of the Office.”

The following checklist is designed to ensure plans developed by Local Providers are consistent with OMH Technical Specifications guidelines with respect to videoconferencing.

Videoconferencing can be characterized by key features: the videoconferencing application, device characteristics, including their mobility, network or connectivity features, and how privacy and security are maintained. The more recent use of desktop and mobile devices requires consideration of each of these. A check mark indicates the plan contains provisions that conform to the standard.

Videoconferencing Applications:

- Applications include appropriate verification, confidentiality, and security parameters necessary to ensure its utilization for this purpose
- Video Software platforms are not in use when they include social media functions or allow others to enter sessions at will

Security and Protection of Data Transmission and Information:

- Steps taken to ensure security measures are in place to protect data and information related to clients/patients from unintended access or disclosure
- Protected Health Information (PHI) and other confidential data is backed up to or stored on secure data storage locations. Cloud services unable to achieve compliance will not be used for PHI or confidential information
- Professionals and patients discuss any intention to record services and how this information is to be stored and how privacy will be protected
- If a mobile device is in use, attention to privacy of information being communicated over this device

- Any information stored on a mobile device is adequately restricted
- Mobile devices will require a passphrase or equivalent security feature. Multi-factor authentication will be used if available
- Mobile devices are configured to utilize an inactivity timeout feature. Timeout does not exceed 15 minutes
- Unauthorized users are not allowed to access sensitive information stored on the device or use the device to access sensitive applications or network resources
- The application includes the ability to remotely disable or wipe mobile device if lost or stolen
- Session logs that are stored by 3rd party location are secure and granted only to authorized personnel
- Videoconferencing software does not allow multiple concurrent sessions to be opened by a single user. If this occurs first session will be logged off or second session blocked
- HIPAA and state privacy requirements will be followed at all times to protect the patient's privacy
- Confidential client/patient data will be encrypted for storage or transmission, and other secure methods shall be utilized, such as safe hardware and software and robust passwords to protect electronically stored or transmitted data
- Network and software security protocols to protect privacy and confidentiality are provided, as well as appropriate user accessibility and authentication protocols
- Measures to safeguard data against intentional and unintentional corruption are in place during storage and transmission
- Security measures are in place to protect and maintain the confidentiality of the data and information relating to clients/patients
- Videoconferencing software capable of blocking provider's caller ID at the request of the provider is utilized

Transmission Speed and Bandwidth:

- Transmission speed is the minimum necessary to allow adequate communications necessary for clinical encounters – (Most protocols use systems that transmit data at a minimum of 384 Kbps)
- Services provide a minimum of 640X360 resolution at 30 frames per second
- Each end point uses bandwidth sufficient to achieve at least the minimum quality shown above during normal operation
- Videoconferencing software should be able to adapt to changes in bandwidth environments without losing connection

- When possible, each party should use the most reliable connection to access the Internet and use wired connections if available

Encryption:

- Encryption (128 bit) of electronic PHI is addressed and video sessions secured consistent with HIPAA and good practices
- Audio and video transmission is secured by using point to point encryption that meets recognized standards (Federal Information processing Standard 140-2 is the US Government security standard used to accredit encryption standards of software and list encryption such as AES as providing acceptable levels of security)
- If data is stored on the hard drive, whole disk encryption to the FIPS standard is used to ensure security and privacy. Re-boot authentication shall also be used
- Recording of services is discussed with patient and encrypted for maximum security. Access is available to authorized personnel only and stored in a secure location

Equipment:

- Equipment used is based on Telecommunication Standard (International Telecommunications Union) which allow for successful conferencing regardless of platform or manufacturer
- Videoconferencing with Personal Computers utilized for VTC complies with all facility state and federal regulations
- Personal Computers have up to date antivirus software and a personal firewall installed. Ensure Personal Computers or mobile devices have the latest security patches and updates applied to operating system and third party applications that may be utilized for this purpose
- When feasible, Personal Computers use professional grade or high quality cameras and audio equipment
- Mobile device management software is utilized to provide consistent oversight of applications, device and data configuration and security of the mobile devices used within the organization
- In the event of disruption, there is an appropriate backup plan in place
- Processes are in place to ensure physical security of equipment and electronic security of data

Additional Comments:

Do you certify: (1) that your organization has read, understands, and will follow Telepsychiatry equipment best practices as outlined by the American Telemedicine Association; (2) that the information submitted on this form is complete and accurate; (3) that you have the equipment installed and operable on site; and (4) that you understand that failure to follow these practices could result in removal of approval of your organization to offer telepsychiatry services?

Yes No

Signature: _____

Title: _____

Date: _____

Reference Material: [The American Telemedicine Association](#)

Created: 9/17/15

Updated: 10/7/15