Telehealth Services During COVID-19 National Emergency
Technical Guidelines Checklist and Attestation for Local Providers

During the COVID-19 national emergency, which also constitutes a nationwide public health emergency, covered health care providers subject to the HIPAA Rules may seek to communicate with patients, and provide telehealth services, through remote communications technologies. Some of these technologies, and the manner in which they are used by HIPAA covered health care providers, may not fully comply with the requirements of the HIPAA Rules.

The following checklist is designed to ensure plans developed by Mental Health Plan Providers are consistent with the Sacramento County Mental Health Plan's Office of Compliance and U.S. Department of Health and Human Services (HHS), Office of Civil Rights (OCR) guidelines with respect to videoconferencing. Videoconferencing can be characterized by key features: the videoconferencing application, device characteristics, including their mobility, and how privacy and security are maintained. A check mark indicates the plan contains provisions that conform to the standard.

Videoconferencing Applications:

☐ In office desktop applications include appropriate verification, confidentiality, and security parameters necessary to ensure its utilization for this purpose.

☐ 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

☐ Covered health care providers using any non-public facing remote communication, have enabled all available encryption and privacy modes when using such applications.

☐ Direct service staff have been notified that public facing applications (Facebook Live, Twitch, Tik Tok and other similar applications) should NOT be used in the provision of telehealth

☐ Direct service provider will be required to inform the client that the use of third-party applications potentially introduces privacy risks

☐ Videoconferencing software capable of blocking provider's caller ID at the request of the provider is utilized

Security and Protection of Data Transmission and Information for Electronic Health Record Remote Use:

☐ Steps taken to ensure security measures are in place to protect data and information related to clients/patients from unintended access or disclosure

☐ Unauthorized users are not allowed to access sensitive information stored on the device or use the device to access sensitive applications or network resources

☐ Complying with HIPAA regulations is always preferable and the Privacy Rule is NOT suspended during this time

☐ Confidential client/patient data will be encrypted for documentation into the client record, 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

☐ Security measures are in place to protect and maintain the confidentiality of the data and information relating to clients/patients

Transmission Speed and Bandwidth:

☐ Transmission speed is the minimum necessary to allow adequate communications necessary for clinical encounters

☐ Each end point uses bandwidth sufficient to achieve at least the minimum quality during normal operation

☐ Videoconferencing software/applications 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

Equipment:

☐ Personal Computers have up to date antivirus software and a personal firewall installed. Ensure Personal Computers 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

☐ Processes are in place to ensure physical security of equipment and electronic security of data

☐ Personal devices should be used only as a last resort and staff should be aware that by using a personal device clients/patients will have access to staff's personal contact information which may be used at will and beyond the current public health crisis.

Do you certify:

1. that your organization will follow Telehealth best practices as outlined by the American Telemedicine Association and direction from Sacramento County Office of Compliance;
2. that the information submitted on this form is complete and accurate;
3. that information has been communicated to staff regarding potential risks of using personal devices to conduct telehealth services;
4. that you have the equipment and testing has been conducted and successful; and
5. that you understand that the change in OCR's enforcement discretion is only effective during the COVID-19 nationwide public health emergency and that the previous regulations will be reinstated at the direction of OCR and Sacramento County Office of Compliance. ☐Yes ☐No

Program Name: _____

Signature and Title: _____

Date: _____