TELEHEALTH GUIDELINES FOR QUALITY ASSURANCE

CLINICAL CONSIDERATIONS FOR TELEHEALTH BEST PRACTICES

- Evaluation for appropriateness of person served to engage in telehealth. Some things to assess functionality, MSE, emotional state, high-risk status regarding suicidality, etc.
- Written informed consent should be required for telehealth services and should be documented in the client's records. Limitations and parameters of telehealth services should be included in the consent.
- Verify a person's location (address, apartment number) at the start of the session in case emergency services need to be engaged.
- Provide information for the Mobile Response Teams and 211 in case the call is disconnected.
    - Clinician / Service Provider should be aware of other providers, resources.
- Request emergency contact information for the person being served.
- Make steps to ensure the client's privacy during the telehealth session as much as possible.
- Prior to the initial telehealth appointment, it is recommended to develop a plan with the person being served for the following events:
    - How to stay on the phone while arranging emergency services (911 or MRT), if needed.
    - Confirm the person's ability to use basic technology and provide information on how to reconnect/next steps in case of a technology failure during the session.
- Telehealth services must use the same standard of maintaining patient medical records as used for in-person services. Medical records must be confidentially maintained, as required in ss. 395.3025(4), F.S.

ADDITIONAL SAFETY AND CRISIS RECOMMENDATIONS

- SAMHSA recommends that all persons served should be screened for suicide at every visit, regardless of their diagnosis or primary reason for treatment.
- It is recommended the Providers use evidence-based tools such as the Patient Health Questionnaire 9 (PHQ-9), the Columbia Suicide Severity Scale (C-SSRS), a risk assessment tool like SAMHSA's SAFE-T Suicide Risk Assessment and/or a validated safety plan such as the Stanley Brown Safety Plan.
    - Link to the Zero Suicide Toolkit at SEFBHN
- In addition to standard risk assessment, assess for the emotional impact of the pandemic on suicide risk.
- Examples that can escalate risk:
    - Increased social isolation;
    - Social conflict for those sheltering together;
    - Increased financial concerns or worry about health or vulnerability in self, friends, and family;
    - Decreased social support;
    - Increased anxiety and fear;
    - Disruption of routines and support.
- Identify protective factors that can be emphasized:
    - Reasons for living (family, hope for the future, children);
    - Deterrents (fear of injury, religious beliefs);
    - Attend to protective factors that may have diminished recently.

- Inquire about increased access to lethal means (particularly stockpiles of Tylenol or medications)

Monitoring and Technical Assistance for Providers

- For monitoring and providing technical assistance (TA) to providers to ensure the best implementation of telehealth across the network:
  - Quarterly TA/info/best practice idea-sharing from all providers to each other and have open discussions on what is working well and what may need improvement
- Regarding monitoring outcomes when it comes to telehealth, some elements to consider are:
  - Retention in treatment, along with basic outcomes per department
  - Consistency and frequency of services
  - Rapport building and techniques to keep individuals engaged via telehealth
- Missed appointments should be tracked, as well as technical issues which caused the session to be interrupted or prevented from starting.
  - In case of missed appointments or technical difficulties, guidelines should be developed regarding plans for rescheduling, as well as a protocol for an alternate plan of communication if there are technical difficulties or issues.
- Mechanisms and evaluations are needed assess clients' satisfaction with tele communication systems.

Technology Considerations & Access to Telehealth Services

- Telehealth should be delivered through pre-approved platform(s).
  - Considerations for multiple platforms to interact with individuals receiving services to accommodate variations in, and difficulties with, technology.
- Adopt a standard expectation around hours of operation and time availability for receiving services via telehealth.
  - Consider mirroring hours of operation; Emergency Services and Screening; Mobile Response Teams
- Training and assistance should be given to staff and people served regarding the use of telehealth: platforms used, troubleshooting, ensuring access, etc. Training topics should cover:
  - EHR compatibility
  - Basic Instructions when using the different platforms to staff
  - Communication to individual served throughout the process of the next steps occurring
  - Keep lag time in mind; minimize distractions
- Differences in service delivery for phone-based telehealth and video telehealth (appropriateness, expectations, etc.)

Supervisory Practices

- While Supervisors may utilize tele-communication systems, including telephone only communication, to conduct Supervisory sessions with staff, it is important for Supervisors and Supervisees to understand the factors that influence the quality and effectiveness of tele-supervision. Therefore, protocols need to be developed to address the following areas surrounding the topic of tele-supervision:

- Informed Consent for utilization of telecommunications systems for the purpose of Supervision.
- Utilization of a HIPPA compliant platform and ensuring that staff are provided with instructions on how to use the chosen platform. Examples of HIPPA compliant platforms are, but not limited to, Zoom, GoToMeeting, Microsoft Teams.
- Contingency planning for managing technical difficulties. Ex. Testing the platform ahead of scheduled Supervision session; obtaining an alternate phone number if there are connectivity issues.
- Confidentiality requirements regarding discussion of client's health protected information in a remote location.
- Professionalism practices and expectations regarding how Supervisors and Supervisees may conduct themselves (i.e. timeliness, distractions, etc.)
- Delivery of needed resources and tools needed by staff to perform their duties and responsibilities.
- Documentation of Supervision sessions

LEGAL AND ETHICAL CONSIDERATIONS

- SAMSHA has shared additional considerations for the use of advanced technologies involving ethical and legal issues: confidentiality, scope of practice, state licensure requirements/regulations, privacy, data security, potential for misuse, and consent management.
- There are extensions in with ethical considerations in Technology Assisted Care in many cases that overlap with ethical considerations in traditional behavioral health services.
- Practitioners need to alert their malpractice insurance carriers of tele behavioral health services to ensure coverage because there might be variations from carrier to carrier.
- Providers should also familiarize themselves with Health Information Technology for Economic and Clinical Health (HITECH) Act. Providers should stay informed of technology changes and updates to utilize the industry's best practices of ensuring confidentiality, tele-behavioral health research findings, and policies.
    - The HITECH Act lays out stronger data security requirements for all health care organizations as well as their business associates. The Act was one of dozens of provisions inserted into the economic stimulus package, known as the American Recovery and Reinvestment Act, in February 2009. It's also known as Title XIII of ARRA.
    - Congress included the beefed-up security provisions in tandem with incentive funds from Medicare and Medicaid to help pay for adoption of electronic health records at hospitals and physician group practices. The intent was to help ensure that as more information is digitized it will remain secure.
    - Enforcement of perhaps the most significant security provision of HITECH, the security breach notification rule, took effect Feb. 22, 2010.
    - An Aug. 24, 2009, Interim Final Rule from the U.S. Department of Health and Human Services spells out security breach notification requirements in more detail. There are several categories to become familiar with such as a 60-day time frame for notification if breach occurs; letters to affected parties via mail; harm thresholds; minimum disclosures necessary; hefty penalties; and individual served ability to request electronic copies of health records.

COVID-19 AND CHANGES TO FEDERAL POLICY

- Office of Civil Rights (OCR) will exercise its enforcement discretion and will not impose penalties for noncompliance with the regulatory requirements under the HIPAA Rules against covered health care providers in connection with the good faith provision of telehealth during the COVID-19 nationwide public health emergency. This notification is effective immediately.
- A covered health care provider that wants to use audio or video communication technology to provide telehealth to patients during the COVID-19 nationwide public health emergency can use any non-public facing remote communication product that is available to communicate with patients. OCR is exercising its enforcement discretion to not impose penalties for noncompliance with the HIPAA Rules in connection with the good faith provision of telehealth using such non-public facing audio or video communication products during the COVID-19 nationwide public health emergency. This exercise of discretion applies to telehealth provided for any reason, regardless of whether the telehealth service is related to the diagnosis and treatment of health conditions related to COVID-19.
- Under this Notice, however, Facebook Live, Twitch, TikTok, and similar video communication applications are public facing, and should not be used in the provision of telehealth by covered health care providers.

POLICIES AND PROCEDURES

- Being specific and consistent about using and defining terms in policy and procedures: telehealth, telebehavioral health, telemedicine, tele-mental health, tele-supervision, etc.
- Policies around procedures regarding:
  - The delivery of telehealth, including location of service provider, privacy; intake and screening; informed consent; confidentiality; clinical practices; risk assessments; treatment planning; discharge planning; termination of services; and ability to transfer services from telehealth to face to face services.
  - Safety planning and emergency or crisis procedures.
  - Protocols to manage challenges, such as technical difficulties.
  - The pre-approved, and HIPAA compliant, platform(s) through which telehealth will be delivered.
- Policies and procedures surrounding monitoring medication and medication compliance:
  - Encouraging open discussions about side effects of medications and medication compliance.
  - Asking to review medication bottles and/or medication storage boxes when medication changes occur. Providers can ask to see medication bottles or medication storage boxes

RESOURCES FOR CONSIDERATION

EVIDENCE BASED PRACTICES FOR TELEHEALTH (SAMHSA)

Telehealth for the Treatment of Serious Mental Illness and Substance Use Disorders | SAMHSA

DCF Telehealth Memo, regarding Baker Acts:

Microsoft Word - Telemedicine FAQ 2-5-13.docx (myflfamilies.com)