

SANILAC COUNTY COMMUNITY MENTAL HEALTH AUTHORITY

ADMINISTRATIVE POLICY

NUMBER: BA168

NAME: COMMUNICATION TECHNOLOGIES

INITIAL APPROVAL DATE:	06/26/2023	BY: Administrative Committee
(LAST) REVISION DATE:		BY:
(LAST) REVIEW DATE:	07/27/2023	BY: Policy Committee
DISCONTINUED DATED:	N/A	REPLACED BY: N/A

I. **PURPOSE**

To ensure that all information and communication technologies used to deliver services at Sanilac County Community Mental Health Authority (Sanilac CMH) meet all applicable goals and standards.

II. **APPLICATION**

Populations: **ALL**

Programs: Eligible Agency staff and contract staff considered for communication technology arrangement. This will vary by department and dependent upon job tasks, duties, and the needs of the individuals they serve.

III. **POLICY**

Sanilac County Community Mental Health Authority (Sanilac CMH) shall establish guidelines for all direct and contracted providers of service to Sanilac CMH individuals when completing job duties in a telehealth/communication technology arrangement.

IV. **DEFINITIONS**

Depending upon the type of program, a variety of terminology may be used to describe the use of information and communication technologies to deliver services, i.e., telepractice, telehealth, telemental health, telerehabilitation, telespeech, etc. The use of information and communication technologies allows providers to use a virtual platform to facilitate interactions visually and auditorily with the individual served, family/support system members, and other providers in/or from remote settings.

- A. Virtual Platform: A form of technology that allows an individual to be seen, heard, and/or interact with a service provider.
- B. Remote Settings: Settings where the individual served, and provider are not in the same physical location.
- C. In-person or Face-to-Face Services: A setting where the service provider and individual being served are in the same physical location.

V. **STANDARDS**

All direct and contracted service providers will be required to meet all applicable legal and ethical standards, including those of Sanilac CMH and its funding, accrediting, and regulatory bodies related to communication technologies use. The standards apply to, but are not limited to, required reporting and documentation, compliance with recipient rights, person centered planning and individual satisfaction, safety, and health.

1. Utilizing communication technologies will be offered as an opportunity for individuals who meet the qualifications and have chosen to use this form for services. The selection of services via communication technologies will be documented through the Telehealth Services Consent form (0528), by checking the box for the type of services that consent is provided for virtually. Verification of this consent will be confirmed verbally with each visit by the service provider and documented in the narrative in the progress note. Informed consent will apply, and individuals reserve the right to revoke consent (Form 0528) at any time.
2. Audio recording, video recording, and photographing the individual served will follow clinical policies for treatment purposes and ensure consent is obtained.
3. The use of communication technology to provide services will be based on a personalized plan for the individual being served. Utilizing communication technologies will not compromise the services being provided, meaning all aspects of care related to face to face services i.e., assessments, planning, monitoring, prevention, intervention, conferencing, follow-up, supervision, education, consultation, and counseling are provided at the same standard of quality virtually as they would be held to face to face.

Initial and ongoing assessments, including any risk assessments, will be conducted. If at anytime a service provider feels that it is no longer safe or effective to deliver services remotely, the decision to utilize the virtual platform will be revisited to address changes in the condition, circumstances of the individual served, the service delivery site, and the need for in-person, and/or face-to-face services.

4. Communication technology-based services will be provided by a virtual platform where the qualifying individual must be able to operate/manage/run the necessary technology to complete the services at the quality level necessary to be compliant with all Agency regulatory and licensing requirements. The standards and expectations for privacy and human dignity, clinical practice guidelines, and safeguarding records of individuals served continue to apply regardless of the virtual platform.
 1. All technology and/or equipment needed for the virtual platform will be available and functional to the IT Security standards in Policy BA013. The equipment will be tested by the service provider and IT staff prior to the start of service delivery. Throughout services the service provider will check and monitor the equipment for any changes, notifying IT of any problems or concerns relating to functionality prior to the service delivery each time.
 2. The individual served will be notified of the equipment needed to perform the services needed to adequately deliver services and communication. If at anytime their ability to operate, or equipment becomes unavailable, the individual will notify Sanilac CMH and their service provider to revisit the options for service delivery at that time.
 3. At the beginning of each service encounter, the provider will confirm with the individual being served, that they are in a location that allows for privileged and confidential information to be disclosed in the virtual platform.
 - a. The service provider will obtain the location specifics. If the current location is not their known address, the provider will acquire where the location is. Gaining this knowledge ahead of time is critical if there is a need for emergency services or crisis intervention. If the provider is unable to identify the location or feels that the location cannot allow for a safe service delivery, it is at the provider's discretion to reschedule or revisit the option for the virtual platform to be used for this and future service delivery.

- b. Prior to the service delivery, the provider will verify the identity of the individual served by asking them to verbalize at least 2 pieces of personal information i.e.) date of birth, address, etc. that can be verified in the patient chart.
- c. The provider will in turn identify themselves and their title.

VI. PRIVACY STANDARDS

Privacy must be maintained during the entire service delivery and applies to both the individual being served and the provider. The service provider will address the importance of privacy and try to help problem solve any compromises of confidentiality by identifying alternatives with the individual. The service provider will ensure that CMH standards are being implemented by following Agency policies as outlined (BA070 and RR040). Identifying a back-up arrangement for communication when a location becomes compromised or if the technology fails will be at the discretion of the service provider and the individual based upon the risk.

VII. STAFF TRAINING

Service delivery through a virtual platform requires CMH staff to receive competency-based training to ensure that the delivery is appropriate and effective. Training should include but is not limited to; human factors (strategies for communication with individuals in remote settings, understanding non-verbal communication, establishing rapport, etc.), crisis response procedures (identifying a crisis situation, implementing a response and reporting/following up on the situation), assessment of risk factors (threats in the location of the individual served, identifying physical hazards, etc.) and how to modify treatment techniques (equipment, materials, interventions, etc.). The training components also encompass how to use the equipment and technology to deliver the services (setup, features, general use, safety considerations, infection control related to the use of technology being shared, basic troubleshooting).

VIII. ENFORCEMENT

All Supervisors are responsible for enforcing this policy. The IT Department, HIPAA Officer, Security Officer, and Recipient Rights Officer will perform audits and enforcement.

IX. REFERENCES

- BA013 – IT Security Policy
- BA038 – Acceptable Use Policy
- BA070 – Communications Policy
- BA152 – Telecommuting/Remote Work Policy
- BC042 – Assessment Policy
- BC142 – Clinical Practice Guidelines
- RR040 – Privacy & Human Dignity
- BA023 – Safeguarding Records of Individuals Served
- Form 0528 - Information and Consent form for Telepsychiatry and Telehealth Services
- RR030 – Informed Consent
- RR003 – Fingerprinting, Photographing, Audio-Recording & Use of One-Way Glass