SANILAC COUNTY COMMUNITY MENTAL HEALTH AUTHORITY

ADMINISTRATIVE POLICY

NUMBER: BA070

NAME: COMMUNICATIONS POLICY

INITIAL APPROVAL DATE:	11/15/2021	BY: Administrative Committee
(LAST) REVISION DATE:	09/23/2024	BY: CIO
(LAST) REVIEW DATE:	10/17/2024	BY: Policy Committee
DISCONTINUED DATE:	N/A	REPLACED BY: N/A

I. PURPOSE

Sanilac CMH has adopted this policy on Communications to comply with HIPAA, with the regulation requirements for such a policy, as well as our duty to protect the confidentiality and integrity of confidential medical information as required by law, professional ethics, and accreditation requirements. All personnel of Sanilac CMH and all facility personnel must be familiar with the contents of this policy and follow its guidance, as appropriate, when using communications technology. Familiarity with the plan and demonstrated competence in the requirements of the plan are an important part of every Sanilac CMH employee's responsibility, as well as that of every other facility employee.

II. APPLICATION

Populations: **ALL**
Programs: **Direct – ALL**
Contracted - ALL

III. POLICY

The Sanilac County Community Mental Health Authority (Sanilac CMH) computing and communication resources are intended for the Sanilac CMH's business purposes and for professional growth through the sharing of information and ideas. It is expected that use of Sanilac CMH's computing and communication resources will fall within the guidelines of generally accepted social and business standards and demonstrate respect for all individuals.

Sanilac CMH has adopted this Communications Policy to comply with HIPAA and the regulations requirement to protect the security of electronic health information, as well as to fulfill our duty to protect the confidentiality and integrity of confidential medical information as required by law, professional ethics, and accreditation requirements. All personnel of Sanilac CMH must be familiar with the policy and demonstrate competence in the requirements of the policy, which is an important part of every Sanilac CMH employee's responsibility.

IV. DEFINITIONS

None.

V. STANDARDS

1. Internet Use:

Sanilac CMH encourages the business use of the Internet to increase productivity. The Internet system and all contents, downloads, anything generated by or handled by the Internet system are part of the business equipment of Sanilac CMH, are owned by the facility, and are not the property of the users of the system.

Consequently, Internet users do not have a right to privacy in their use of the computer system or the Internet component. Sanilac CMH reserves the right to monitor, audit, delete, and read anything pertaining to Internet usage. It is the policy of Sanilac CMH to regularly monitor the contents of Internet usage; it may monitor the contents and usage to support operational, maintenance, auditing, security, and investigative activities.

Users should use the Internet with the knowledge that Sanilac CMH may from time to time examine the content or trail of Internet usage. Sanilac CMH cannot guarantee that Internet usage will be private. Use of the Internet constitutes consent to this policy. Generally, Internet users should restrict their use of the Internet system to proper business purposes relating to the care and treatment of individuals we serve and related administrative matters, such as looking up Board Association information. A user may, however, use the Internet for personal purposes, under the following conditions:

- Personal use does not involve significant use of the facility's resources, such as work time, computer time, excessive bandwidth, costs and the like, and does not preempt any business activity or interfere with the user or other's productivity.

- Users must not transmit confidential or proprietary information to unauthorized recipients. Proprietary information is information that belongs to Sanilac CMH.

- Users must not access sites that contain obscene, pornographic, offensive, harassing, or hostile material. No person shall enter, transmit, or maintain sites with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, sexual preference, or health condition. No person shall enter, maintain, or access sites with any abusive, profane, or offensive language. Some filters have been put into place to help block offensive material from being viewed by any staff member.

- Users will not download material that is not business related or approved by the IT Department. Users must report any possible virus-like activity to the IT Department immediately.

- Internet usage must not involve any illegal or unethical activity.

- Internet usage must not involve or disclose any activity that could adversely affect Sanilac CMH, its officers, employees, or agents.

- Internet usage must not involve solicitation. Employees may not use the facility's Internet system to solicit for outside business ventures, organizational campaigns, or political or religious causes.

The IT Department shall provide access to Internet services for those employees who need such access to perform their job duties. This access may be through the employee's individual

workstation or may be through a centrally placed Internet port. The request for access to Internet services will be made to their Department Supervisor, with access set up by the IT Department. Sites visited and time logged on the Internet will be provided to supervisors or chiefs upon request. Passwords are to be kept confidential.

A variety of sites are potentially destructive to the security of Sanilac CMH's Information System(s), including the possibility of attacks on the Information System(s), serious bandwidth degradation, and harm to individual workstations. Because of this, users are not permitted to download software or computer enhancements, such as MP3's, iTunes, etc. Users are permitted to download manuals or data that pertain to their conducting day-to-day business.

Users must immediately report violations of this policy to their supervisor and to the CIO.

2. Email Use:

Sanilac CMH encourages the business use of e-mail to increase productivity. The e-mail system and all messages generated by or handled by e-mail, including backup copies, are part of the business equipment of Sanilac CMH, are owned by the facility, and are not the property of the users of the system. Consequently, e-mail users do not have a right to privacy in their use of the computer system or its e-mail component. Sanilac CMH reserves the right to monitor, audit, delete and read e-mail messages. The CIO or designee may override user passwords. Although it is the policy of Sanilac CMH to not regularly monitor the contents of e-mail communications, it may monitor the contents and usage to support operational, maintenance, auditing, security, and investigative activities. Users should use email with the knowledge that Sanilac CMH may from time to time examine the content of e-mail communications and will not guarantee that email messages will be private. E-mail communications can be forwarded, intercepted, printed, and stored by others. Use of the e-mail system constitutes consent to this policy.

Generally, e-mail users should restrict their use of the e-mail system to proper business purposes relating to the care and treatment of individuals and related administrative matters, such as billing. If the electronic mail is used for personal reasons, it is to be used with the following conditions:

- Personal use does not occur during working hours, unless during breaks or lunch.

- Users must not transmit confidential or proprietary information to unauthorized recipients. Proprietary information is information that belongs to Sanilac CMH.

- Users must not transmit obscene, offensive, harassing, or hostile messages to any recipient. No person shall enter, transmit, or maintain messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, sexual preference, or health condition. No person shall enter, maintain, or transmit any abusive, profane, or offensive language.

- Electronic mail attachments will be scanned automatically with the system's antivirus software prior to opening the attachment. Users must report any possible virus like activity to the IT Department immediately. Users will not open e-mail attachments that are not business related.

- Transmission must not involve any illegal or unethical activity.

- Transmission must not involve or disclose any activity that could adversely affect Sanilac CMH, its officers, employees, or agents.

- Transmission must not involve solicitation. Employees may not use the facility's e-mail system to solicit for outside business ventures, organizational campaigns, or political or religious causes.

- The e-mail system will employ user IDs and associated passwords to isolate the communications of different users. Users must never share passwords or reveal them to anyone else. If users must share data, they must use message-forwarding facilities, group profile directories on local area network servers, and other authorized information sharing mechanisms. Employees may not intercept or disclose or assist in intercepting and disclosing e-mail communications.

- Because some information is intended for specific individuals and may not be appropriate for general distribution, users should exercise caution when forwarding messages. Users must not forward sensitive information, including individuals served information (refer to Safeguarding Records of Individuals Served Policy #BA023 for list of De-Identified Information), to any party outside the Sanilac CMH system without prior approval of the department supervisor or the CIO. Senders may not engage in blanket forwarding of messages to parties outside the Sanilac CMH system unless the sender has obtained the prior permission of the CIO.

- Users should periodically purge email that is no longer needed for business purposes. Users should empty the Deleted Items folder on a regular basis.

- Sanilac CMH will make all e-mail messages sent or received that concern the diagnosis or treatment of an individual part of that individual's medical record and will treat such e-mail messages with the same degree of confidentiality as other parts of the medical record. The COO or CIO will review and determine whether particular e-mail messages will constitute part of an individual's medical record.

- Persons that we serve must consent to the use of e-mail for confidential medical information. They must sign a consent form that will become a part of their medical record. This consent form must include disclosures detailing the risks of email and identifying information on the internet.

- All e-mail concerning individuals served information must include the Agency confidentiality statement.

- All email correspondence with individuals will become part of his/her medical record.

- Along with authorization provided via the consent form, Agency staff and system users must de-identify persons served when sending emails. Use of full names, social security numbers, diagnosis, etc. is not permitted (refer to Safeguarding Information of Individuals Served Policy #BA023 for list of De-Identified Information). If email communication of protected and/or confidential information is required, encryption must be applied and used without exception during ongoing communications with the individual.

- Sending, forwarding, and copying emails to unintended and/or unauthorized recipients; internal or external is prohibited.

- Sending, forwarding, and copying non-encrypted emails (including accidentally) that contain identifying and/or confidential information outside of the CMH internal computer network will result in disciplinary action including termination (refer to Safeguarding Records of Individuals Served Policy #BA023 for list of De-Identified Information).

- All emails may be discoverable in litigation regardless of whether it is in an individual's medical records.

- Sending or forwarding email that is considered spam, chain letters, or junk mail is not acceptable business practices.

- All staff that are unable to respond to emails timely are required to configure an out of office auto-response for the duration of scheduled time off.

- All staff are required to have a uniform signature line on email responses which is to include only the following items:

  First and last name and credentials (i.e.: LMSW, MBA, LLPC, etc.)
  Position(s)
  Sanilac County Community Mental Health Authority
  Staff member's direct phone number or the Agency's main phone number
  Agency fax number
  Agency Logo with Mission Statement
  Confidentiality statement:

  The information in this e-mail, including any attachments, might contain information that is privileged, confidential, and/or otherwise exempt from disclosure under applicable law. Any files transmitted with it are the property of Sanilac County Community Mental Health Authority. This e-mail and all attached documents are intended solely for the addressee, access to this e-mail by anyone else is unauthorized. If you are not the intended recipient, any disclosure, copying, distribution or any action taken in reliance on it, is prohibited and may be unlawful. If you believe that you have received this e-mail in error, please contact the sender, indicating you are not the intended recipient and immediately destroy all copies of this e-mail. Receipt by anyone other than the intended recipient is not a waiver of any privileged information. This message has been prepared on resources owned by Sanilac County Community Mental Health Authority – Sandusky, Michigan.

- The addition of pronouns is strictly the choice of staff in the following format only, without any link: Pronouns: He/Him/His or She/Her/Hers or They/Them/Theirs. Any staff member who lists their personal pronouns need to be able to explain what this means if asked.

- Email stationery setting themes are not permitted.

- All emails sent are part of business for Sanilac CMH and should be professional in appearance.

- Users must immediately report violations of this policy to their supervisor and to the CIO.

3. Cellular Devices:

The Sanilac CMH cellular telephones are intended for Sanilac CMH business purposes and for professional growth through the sharing of information and ideas. It is expected that use of these cellular telephones will fall within the guidelines of generally accepted social and business standards and demonstrate respect for all individuals. The usage of cellular telephones is to assist in conducting day-to-day business.

- Cellular telephone users should restrict their use of the cellular phone to proper business purposes relating to the care and treatment of individuals and related administrative matters, such as an employee calling in to their supervisor for direction.

- Users must not transmit confidential or sensitive information while using a cellular telephone, such as use of full names or addresses, or other identifying information; unless an emergency is occurring, or time sensitive information is necessary for the safety or immediate well-being of the individual**.** (Refer to Safeguarding Records of Individuals Served Policy #BA023 for list of De-Identified Information).

- Users must not transmit obscene, offensive, harassing, or hostile messages to any recipient. No person shall discuss issues with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, sexual preference, or health condition. No person shall transmit any abusive, profane, or offensive language.

- Use of cellular telephones must not involve any illegal or unethical activity. Use of cellular telephones must not involve or disclose any activity that could adversely affect Sanilac CMH, its officers, employees, or agents.

- Use of cellular telephones must not involve solicitation. Employees must not use the facility's cellular phones to solicit for outside business ventures, organizational campaigns, or political or religious causes.

- Cellular devices are not to be used while driving. If you receive a call or need to make a call while driving, you need to pull over to the side of the road and stop the vehicle first before you dial the telephone.

- In the event that unauthorized use is suspected, or the cellular device is lost or stolen, it must be brought to the attention of the IT Department and your direct supervisor immediately.

- The device may be wiped clean to ensure sensitive data is removed from the device.

Personal Cell Phones

- Staff who opt to use their personal cell phone for Agency business must sign the #0532 form and obtain their supervisor's and HR approval. Use of a personal cell phone for business use without a completed #0532 form is strictly prohibited.

- The use of a personal cell phone is meant for phone calls only, however, if text messaging is necessary, prior approval must be obtained from the staff's supervisor.

- Internet access for business use is limited to a select number of staff primarily under the supervision of the CIO.

- Personal cell phone use for business must be locked with a passcode, biometric and/or secure device locks to prevent unauthorized access when not in use. Passwords must be at least 8 characters long.

- Any type of privacy breach or suspected breach with the use of a personal cell phone must be reported to your supervisor immediately and the CIO.

- Upon separation from the Agency, personal cell phones used for Agency business must be provided to the IT Department to verify that no Agency-related information exists on the cell phone.

Agency Cell Phones

Cellular telephone conversations are broadcast over airwaves and can potentially be received by many unintended recipients.

- Cellular telephone equipment is part of Sanilac CMH's business equipment.

- **Agency cell phones are not for personal use.** The only exception allowed is for emergencies. If this situation occurs, make your supervisor aware of the incident.

- Cell phones will be issued to any staff, as their supervisor deems necessary. Your supervisor must contact the IT Department to be issued an Agency cellular telephone or to have one of them fixed.

- Agency Cell phones must be password protected. Passwords will be set up by the IT Department. Staff are not permitted to change the assigned password.

- Any type of privacy breach or suspected breach on an Agency cell phone must be reported to your supervisor immediately and CIO. An example of this would be an individual, or non-employee using an unlocked phone.

- The employee will not misuse an Agency cell phone. Misuse includes personal use. This will result first in a written warning, which will also be placed in the employee's personnel file. If the misuse continues after the written warning, the cellular telephone will be taken from the staff member. After an employee loses the privilege of their assigned cellular telephone, they will not be able to utilize another staff member's cellular telephone. Refer to the Agency Discipline/Sanction Policy BA044.

- Replacements: If for any reason a cellular telephone is lost or damaged, the Agency will replace up to two (2) cellular telephones. The third and subsequent units will be replaced at the staff's expense and will be property of Sanilac CMH.

Text Messaging

- Text Messaging is permitted with Supervisor approval for Agency business on Agency or personal cellphones.

- Authorized users must de-identify recipients and patient information. No confidential information can be sent or received via text messaging (refer to Safeguarding Records of Individuals Served Policy #BA023 for a list of De-Identified Information).

- Texting is not permitted while driving in Agency or personal vehicles.

- Persons that we serve must consent to the use of text messaging to communicate with Sanilac CMH staff. They must sign a consent form that will become a part of their medical record. This consent form must include disclosures detailing the risks of texting and identifying information and how this information may be at risk. If an individual initiates text communication with staff, no response or communication is permitted via text until the consent form is signed and processed.

- When text messaging with individuals we serve, it should always be treated as insecure and no identifiable PHI or confidential information should be used (refer to Safeguarding Records of Individuals Served Policy # BA023 for list of De-Identified Information). No information is to be shared with anyone outside of the Agency unless pre-authorized with a court order or other legal means.

- When text messaging with individuals we serve, the text messages should be deleted as soon as the conversation has completed, or no more than 24 hours from the initial communication. No text messages should be stored on Agency or personal cell phones for historical purposes.

4. Fax Machines

- Reasonable care should be used when releasing information via the fax machine to assure confidentiality is maintained.

- The staff responsible for transmitting the facsimile will assure in advance that someone is available to receive and/or is expecting to receive the facsimile.

- All facsimile documents containing clinical or confidential information being sent outside the Agency will utilize a standard format (Form #0077) containing the following statement:

  CONFIDENTIAL - Unless otherwise indicated or obvious from the transmittal, the information contained in this facsimile message is privileged and confidential information intended for the individual or entity named above. If the reader of this message is not the intended recipient, but the employee or agent responsible to deliver it to the intended recipient, you are hereby notified that any dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this communication in error, please notify us by telephone, and return the original message to us at the above address via the U.S. Postal Service at our expense. Thank you."

- Whenever feasible, information regarding individuals will utilize case numbers or other mechanisms that reduce identification of the individual to further protect confidentiality (refer to Safeguarding Records of Individuals served Policy #BA023 for list of De-Identified Information).

- The staff transmitting the facsimile will produce a confirmation document on the facsimile machine as a further check to assure that the information has reached the

intended recipient.

- Each site's fax machine will be monitored closely by the Program Secretary to ensure confidential material is not left unattended in the fax machine for a long time. Faxes will be distributed to the intended staff member as soon as possible after the fax is received.

VI. ENFORCEMENT

All supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination from employment, professional discipline, or criminal prosecution in accordance with the facility's Sanction Policy.

VII. ATTACHMENTS

VIII. REFERENCES

BA023 Safeguarding Records of Individuals Served
0532 Sanilac CMH Agency Cell Phone Usage