SANILAC COUNTY COMMUNITY MENTAL HEALTH AUTHORITY

ADMINISTRATIVE POLICY

NUMBER: BA023

NAME: SAFEGUARDING RECORDS OF INDIVIDUALS SERVED

INITIAL APPROVAL DATE:	03/12/2008	BY: Administrative Committee
(LAST) REVISION DATE:	12/15/2022	BY: CIO
(LAST) REVIEW DATE:	12/14/2023	BY: Policy Committee
DISCONTINUED DATE:	NA	REPLACED BY: NA

I. PURPOSE

The purpose of this policy is to ensure that the records of individuals served by Sanilac County Community Mental Health Authority (Sanilac CMH) are secure and safeguarded against any foreseeable or perceived threat or breach of confidentiality, misuse, and misplacement.

II. APPLICATION

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

III. DEFINITIONS

A. Electronic Health Record: Also known as EHR, shall refer to the protected health information of individuals served by Sanilac CMH and maintained in an electronic format and stored in computer files, in an EHR software system and on the servers of the Agency. This would be any protected health information generated on and after October 1, 2007.

B. Individual: Individual shall mean any individual who is receiving or has received services from Sanilac CMH.

C. Paper Record: Paper record shall refer to the protected health information of individuals served by Sanilac CMH has been scanned to an electronic format with a list maintained by the Clinical Records Secretary.

IV. POLICY

The records of the individuals we serve are considered the physical property of the Agency. The information contained therein is the property of the individual and may be released only as set forth in agency policy RR005 - Confidentiality and Disclosure of Information.

V. STANDARDS

1. The Chief Information Officer (CIO) is responsible for policies and procedures pertaining to the records of the individuals we serve. The safety of the record that is stored electronically in computer files, in the EHR software system or on servers will be assured by the agency's IT and Data Management procedures and staff, and these records will be accessible only through a password protected process.

2. Only staff and contract agency employees of Sanilac CMH may access an individual's record, and access should be on a need-to-know basis and limited to purposes related to planning/providing treatment, documentation of services, billing and/or auditing.
3. If an individual, guardian or parent with legal custody of an individual wishes to review their record, an appointment should be made within one (1) week of the request and all of the individual's records made available. A Sanilac CMH staff will be present while the record is being reviewed in order to assure the record is not breached in any way. Refer to the Confidentiality and Disclosure of Information Policy (#RR005) regarding the release of confidential and/or privileged information.
4. Individual records can only be released under specific circumstances and with a valid release of information (MDHHS 5515). Refer to the Confidentiality and Disclosure of Information Policy (#RR005) and the Responding to Subpoenas and Search Warrants Procedure (#RR1017) regarding the requirements/standards for releasing an individual's record.
5. The Clinical Records Secretary shall be responsible for the integrity and safety of the record.
6. Whenever feasible, information regarding individuals we serve will utilize case numbers or other mechanisms that reduce identification of the individual further protecting an individual's confidentiality.
7. Disclosures of De-Identified Information
   a. Sanilac CMH may freely use and disclose de-identified information. De-identified information is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. De-Identification can be achieved by removing 18 specific identifiers.

      The 18 specific elements listed below relating to the individual, employee, relatives, or employer must be removed, and staff must be certain there is no other available information that could be used alone or in combination to identify an individual.

      1. Names
      2. Geographic subdivisions smaller than a state
      3. All elements of dates (except year 0 related to an individual – including dates of admission, discharge, birth, death – for persons > 89 years old, the year of birth cannot be used
      4. Telephone numbers
      5. FAX numbers
      6. Electronic mail addresses
      7. Social Security Number
      8. Medical Record numbers
      9. Health plan beneficiary numbers
      10. Account numbers
      11. Certificate/license numbers
      12. Vehicle identifiers and serial numbers including license plates
      13. Device identifiers and serial numbers
      14. Web URLs
      15. Internet Protocol (IP) addresses
      16. Biometric identifiers, including finger and voice prints
      17. Full face photos and comparable images
      18. Any unique identifying number, characteristic or code

      Staff must determine that the risk is very small that the information could be used alone

or in combination with other reasonably available information by an anticipated recipient to identify the individual.

8. Information collected on individuals we serve must be accurate, timely, complete and available within the individual's record when needed.
9. All staff will handle any individual's information in a secure fashion; log off of workstations when not in use; secure materials away when not being worked on; secure interoffice mail in confidential envelopes; put away/secure an individual's information when left temporarily; staff should not leave any information unattended or fax any identifiable information unless it is an emergency. Physical safeguards include locking doors and/or filing cabinets and accessing PHI by using their own login information.
10. When a document with any individual's information has to be transported by staff from one agency site to another, or to any other location, the record must be secured in an agency mail bag that is locked. Any vehicle used to transport agency information or information on individuals we serve must be locked when unattended. No information should be left in a vehicle overnight.

VI. ATTACHMENTS

None

VII. REFERENCES:

Please reference the following policies and procedures for further direction on Medical Records:

- BA004 Medical Record Policy
- BA070 Communications Policy
- RR005 Confidentiality and Disclosure of Information
- RR1017 Responding to Subpoenas and Search Warrants