

SANILAC COUNTY COMMUNITY MENTAL HEALTH AUTHORITY

ADMINISTRATIVE POLICY

NUMBER: BA170

NAME: SURVEILLANCE (RECORDED/NON-RECORDED) POLICY

INITIAL APPROVAL DATE:	(Planning)	BY: Administrative Committee
(LAST) REVISION DATE:		BY:
(LAST) REVIEW DATE:	04/18/2024	BY: Policy Committee
DISCONTINUED DATE:	N/A	REPLACED BY: N/A

I. **PURPOSE**

Sanilac CMH has adopted this policy on surveillance to comply with the regulation requirements of the Michigan Mental Health Code in relation to this policy, as well as our duty to the individuals we serve as required by law, professional ethics, and accreditation requirements. All personnel of Sanilac CMH must be familiar with the contents of this policy and follow its guidance, as appropriate. Familiarity with the policy and demonstrated competence in the requirements of the policy are an important part of every Sanilac CMH employee's responsibility.

II. **APPLICATION**

Populations: **All**
Programs: **Direct - All**
Contracted - All

III. **POLICY**

The Sanilac County Community Mental Health Authority (Sanilac CMH) surveillance resources, whether recorded or non-recorded, are intended for Sanilac CMH business purposes and for protection of the individuals we serve, our staff, the Agency, and our community. It is expected that use of the Sanilac CMH recorded/non-recorded surveillance resources will follow strict guidelines put into place by the Michigan Mental Health Code, federal/state regulations, contract requirements, our accreditation body, and specific definitions within this policy.

IV. **STANDARDS**

Consistent with the Michigan Mental Health Code, Sanilac CMH may conduct recorded/non-recorded surveillance for purposes of safety, security, and quality improvement. Recorded/non-recorded surveillance may only be conducted in common areas such as hallways, entrance ways, etc. Recorded surveillance is occurring on the exterior of CMH buildings and into the public parking lots.

- A. Visible and obvious signage indicating active recording surveillance will be posted in areas where surveillance monitoring occurs.
- B. Monitors will be hung in the main clerical support offices at the Ehardt building and Administration building. A floor plan denoting the location of surveillance equipment will be maintained.
- C. Recording of surveillance will only be allowed with the cameras affixed to the exterior of the buildings. Recordings will be housed on a server for a maximum of 30 days. If notice is received that an incident requires investigation by the Department's Office of Recipient Rights, the Licensing division of the Bureau of Community and Health Systems, law enforcement, licensed psychiatric

hospital or Unit Office of Recipient Rights, and/or the United States Department of Health and Human Services Centers for Medicaid and Medicare Services, the footage will be retained for the duration of the investigation.

- D. Interior vestibule and hallway cameras will be non-recording surveillance only. NO EXCEPTIONS.
- E. Requests to view:
 - a. Requests must be made within 7 days of an incident to be considered.
 - b. Requests must be made in writing to the CIO.
 - c. Requests can only be made for viewing of the exterior cameras as the interior cameras are a live feed only.
 - d. If more than one individual is viewable during the incident, requests to review recordings will only be approved for the Office of Recipient Rights, Human Resources, or law enforcement who need to view the occurrence as part of an investigation.
 - e. Viewing will not be permitted without a signed consent from all individuals that are present in recorded footage, except for requests from the Office of Recipient Rights, Human Resources or law enforcement, who have unimpeded access while completing an investigation.
 - f. Requests must indicate the incident in question. Non-specific requests to view recorded surveillance will not be considered.
 - Incidents include (but are not limited to):
 - a. Falls
 - b. Fights
 - c. Accidents
 - d. Theft
 - e. Vandalism
 - f. Vehicle Damage
 - g. Destruction of Property
 - g. Access to recorded surveillance is monitored monthly, or as requested, through review of the audit log in DW Spectrum. The audit log shows viewer's name, date and time of access, and date and time of event. In addition, a record will be kept that will reference any complaint or investigation information involved in viewing.
- F. Requests for copies:
 - a. Requests must be made within 7 days of an incident to be considered.
 - b. Requests must be made in writing to the CIO.
 - c. Requests can only be made for copies of the exterior cameras as the interior cameras are a live feed only.
 - d. If more than one individual is viewable during the incident; requests will only be approved from the Office of Recipient Rights, Human Resources or law enforcement who need a copy of the occurrence as part of an investigation.
 - e. A copy cannot be released without a signed consent from all individuals that are present in the video footage, except for requests from the Office of Recipient Rights, Human Resources, or law enforcement, who have unimpeded access while completing an investigation.
- G. FOIA: Video surveillance recordings are not deemed a public record and would be exempt from being acquired under the Freedom of Information Act. Legal opinion will be sought when a FOIA request is received to ensure an exception isn't appropriate.
- H. Recorded surveillance images shall not be maintained as part of a recipient's clinical record.
- I. Requests for an exception to this policy can be made in writing through the RRO and the CEO.

V. **DEFINITIONS**

- Consent: Signed release from an individual, guardian, or parent of a minor that specifies what information is allowed to be shared and whom it can be shared with.

VI. **PROCEDURE**

REQUEST TO VIEW PROCESS

1. A request to view the recorded surveillance can come from an individual, a parent (of a minor) or guardian, law enforcement, RRO, MDHHS, or a staff member.
2. The request must be made in writing within 7 days of the incident and contain:
 - a. Date of incident
 - b. Name of requester
 - c. Reason for request
 - d. Contact information
3. Request should be submitted to the CIO.
4. The CIO will log the request.
5. The CIO will discuss with the CEO and/or COO the request to determine if appropriate.
6. The CIO will reach out to requester and either explain why viewing is not appropriate or set up time for viewing of recorded surveillance.
7. The CIO will document the viewing.

REQUEST FOR COPY PROCESS

1. A request for a recorded surveillance copy can come from an individual, a parent (of a minor) or guardian, law enforcement, RRO, MDHHS, or a staff member.
2. The request must be made in writing within 7 days of the incident and contain:
 - a. Date of incident
 - b. Name of requester
 - c. Reason for request
 - d. Contact information
 - e. A signed guarantee that no unauthorized distribution of the copy will be made.
3. Request should be submitted to the CIO.
4. The CIO will log the request.
5. The CIO will discuss with the CEO and/or COO the request to determine if appropriate.
6. The CIO will reach out to requester and either explain why a copy will not be made or make arrangements for pick-up of the recorded surveillance copy.
7. For court orders, the CIO will ensure that the copy is provided within 10 calendar days of the request or sooner.
8. The CIO will document the distribution of the recorded surveillance.

EXCEPTIONS

Requests for an exception to this policy can be made in writing through the RRO and the CEO.

VII. **ENFORCEMENT**

All Supervisors are responsible for enforcing this policy. The IT Department, Recipient Rights Officer and Security Officer will investigate complaints. 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 Agency's Sanction Policy.

VIII. ATTACHMENTS

IX. REFERENCES