SUBJECT: Security Camera and Digital Recording	*PAGE*: 1 of 4
SERVICE LINE OWNER: Superintendent	*Date: 4/12/21*

Purpose

To outline the use of security/surveillance cameras and Network Video Recording (NVR) equipment utilized at the Glenwood Resource Center (GRC) and to establish procedures for creating, maintaining, storing, and releasing video evidence obtained from the use of security/surveillance cameras and NVR systems. Because the video information records DHS services being delivered to individuals with medical needs, it is protected confidential information.

Policy

It is the policy of the GRC to place security/surveillance cameras within the common areas of identified homes and worksites to ensure individual and staff safety. Reasonable steps will be taken to protect the privacy of the individuals living at GRC and to minimize the number of GRC staff with access to video data. Control of security/surveillance cameras, NVR equipment, and video evidence shall be the responsibility of the GRC Superintendent or designee. Procedures pertaining to the control of security/surveillance camera video data shall follow the guidelines established in this policy. No protected health information (PHI) shall be released without proper authorization. When using, requesting, or disclosing PHI, reasonable efforts shall be made to limit PHI to the minimum necessary to accomplish the intended purposes of the use, disclosure, or request.

Definitions

"Security/Surveillance Cameras": An integrated system of cameras and monitoring equipment placed strategically within homes and worksites at the facility. Cameras will only monitor video image with no audio.

"**Individual**": Means any minor or dependent adult residing at and receiving services from a resource center. For the policies on human rights and abuse, it also includes any minor or dependent adult not residing at but receiving services from a resource center.

"Incident": Means any action, situation, behavior, or occurrence that is not consistent with the care, treatment, or habilitation plan of an individual or that may affect the health or safety of the individual.

"Network Video Recorder (NVR)": A specialized computer system that includes software designed to electronically record a series of digital images to a designated network storage system. Images are stored for a pre-determined amount of time.

"Masked video": A portion of a video image that is hidden from the viewer to protect the privacy of the individual on video (e.g. bedrooms and bathrooms).

Procedure

Parental/guardian verbal consent and Human Rights Committee (HRC) review and approval must be obtained prior to the use of security/surveillance cameras and NVR equipment. Written

parental/guardian consent must be obtained within thirty (30) days of verbal consent. Parental/guardian consent and HRC approval is time limited and must be renewed annually.

Placement of Security/Surveillance Cameras:

Security/surveillance cameras will be placed within identified homes and worksites to ensure individual and staff safety. Security/surveillance cameras will be placed in the common areas of the home (e.g. living room, dining room, kitchen, hallways). No security/surveillance cameras or equipment shall monitor areas where individuals, staff, or visitors have a reasonable expectation of privacy such as bedrooms, bathrooms, or shower areas. Video images of all common areas will be recorded to a NVR.

Signage will be located on the entrances of the homes and worksites to notify persons entering the homes that cameras are in use.

Access and Monitoring of Security/Surveillance Cameras or Video Data:

Individuals, staff, and visitors are prohibited from unauthorized use, tampering with, or otherwise interfering with security/surveillance cameras/equipment or video data, and will be subject to appropriate disciplinary and/or criminal action depending on the severity of their actions.

Security/surveillance cameras and will be operated and monitored by the GRC Superintendent or designee, Assistant Superintendent of Program Services, and Assistant Superintendent of Integrated Services as the only individuals authorized to access the NVR system. The GRC Superintendent or designee is responsible for establishing additional users on the NVR system. GRC Management Information Services (MIS) and GRC maintenance staff may also have limited access based on job specific responsibilities.

Any issues with the security/surveillance cameras or NVR systems should be reported immediately to the GRC Superintendent or designee, Assistant Superintendent of Program Services, or Assistant Superintendent of Integrated Services for immediate resolution.

Storage and Retention of Security/Surveillance Camera Video Data

The GRC Superintendent or designee, Assistant Superintendent of Program Services, and Assistant Superintendent of Integrated Services have the authority for archiving security/surveillance camera video data, establishing users on the NVR system, and maintaining archived security/surveillance camera video data.

Security/surveillance cameras are set to record data twenty-four (24) hours a day, seven (7) days a week within the limitations of the system capabilities (e.g. digital recording space, power disruptions, serviceability, and maintenance).

Video data will be stored on the NVR for thirty (30) days. If there is data of significance (e.g. data related to a specific reported or suspected incident), that data must be exported and archived (transferred to a dedicated internal network storage location). If the data is not archived within the thirty (30) day time period, new recordings will be recorded in the available space and older material will no longer exist. All exported and archived security/surveillance camera video data not stored and maintained for evidentiary purposes under this policy shall be disposed of

by the GRC Superintendent or designee in a manner that ensures the contents are not retrievable.

Review of Security/Surveillance Camera Video Data

Information obtained through the use of the security/surveillance cameras and NVR equipment may only be used for the purpose(s) outlined in this policy and must be related to the protection and safety of individuals, staff, and/or the public/visitors, including discipline or the consequences that arise from that, or it must assist in the detection and deterrence of abuse, neglect and criminal activity. Information should not be retained or used for any other purposes other than that described in this policy.

Security/surveillance video data will be reviewed when there is a need to do so either because an incident has been reported or is suspected to have occurred. Examples of incidents to be reviewed include, but are not limited to, allegations of abuse, any incident where staff are called to respond, an incident resulting in individual and/or staff injuries, and similar events that may involve supervisory follow-up.

Staff must receive written permission from the GRC Superintendent or designee, Assistant Superintendent of Program Services, or Assistant Superintendent of Integrated Services in order to review security/surveillance camera video data. Requests for reviewing security/surveillance camera video data will be limited to those staff who have a direct interest or "need to know" regarding the incident under review. Only the portion of the security/surveillance camera video data concerning the specific incident will be available for viewing. Not all requests will be granted and will be based on individual circumstances. If the request is granted, an appointment will be set up with the GRC Superintendent or designee to review security/surveillance video data. The GRC Superintendent or designee shall have final authority regarding approval or denial of security/surveillance video data review should any dispute arise.

External law enforcement personnel (acting within the scope of their duties) may be authorized to review security/surveillance camera video data on internal GRC systems at the GRC facility. Staff are expected to assist external law enforcement personnel in the review process.

Iowa Department of Inspections and Appeals (DIA) personnel (acting within the scope of their duties) may be authorized to review security/surveillance camera video data on internal GRC systems at the GRC facility. Staff are expected to assist DIA personnel in the review process.

Release of Security/Surveillance Camera Video Data

To maintain the evidentiary value of NVR recordings, security/surveillance camera video data shall only be archived with software that is proprietary to the system it was originated on. The formatting should not be changed. Under no circumstances should security/surveillance cameras video data/images be transmitted via other media (e.g. cell phone text message).

Security/surveillance camera video data will typically remain internal information/data, but may be released to outside parties under the following guidelines:

- To assist external law enforcement personnel during the course of an investigation, pursuant to a subpoena, and

- To provide evidence to assist external law enforcement personnel or prosecutors in any criminal proceedings, pursuant to a subpoena.

Privacy and Security/Surveillance Camera Video Data

Certain images on the NVR recording system may be "masked" in an effort to protect individual privacy. The GRC Superintendent or designee, Assistant Superintendent of Program Services, and Assistant Superintendent of Integrated Services shall have the ability to view all Security/Surveillance Cameras and are the only staff authorized to review.

Training

All employees shall receive training on this policy and annually thereafter. All new employees will receive training on this policy in New Employee Orientation. All training shall be documented in staff's training record.

Quality Assurance

Supervisors and management staff will monitor for compliance.

Marsha Edgington, Superintendent
4/12/21