Security Systems and Protocols

Personal Alarm Systems

The Personal Alarm System (PAS) identifies and tracks the location of individuals in need of assistance. PAS communicates via radio frequencies from a transmitter/personal alarm device issued to designated facility personnel to computer workstations located in the Control Room.

PAS transmitters are assigned to designated facility personnel, i.e., individuals whose responsibilities require direct interaction with the client population. Safety is responsible for programming and issuing transmitters to designated facility personnel.

The PAS transmitter is to be activated only when a staff person is in a situation, or witnesses a situation, that poses an imminent threat to the safety of clients and/or staff members.

Other personnel, as authorized by the facility, shall be issued a PAS transmitter if deemed necessary for the performance of their assignment. PAS transmitters are secured and carried on lanyards provided by the facility or, on key rings with facility-issued keys.

Facilities with coverage in parking lots/parking garages will issue a PAS device to all employees.

The Chief Safety Officer, in conjunction with the Environment of Care Committee (EOCC), will develop a policy and procedure for the implementation of the PAS equipment. Safety, direct care and direct support staff, will be trained in the use of the PAS equipment. All approved PAS applications shall be incorporated into the Facility Security Management Program. Training shall be made available to new hires and follow-up training pursuant to facility policy.

PAS coverage will be provided for all inpatient buildings and locations that provide programming and/or services for inpatient clients. **PAS coverage may be extended to parking lots/garages and other areas of a campus, but only based on approval by the Administrative Support Services Group (ASSG).** Spell out what ASSG is prior to using an acronym

The Safety Department is responsible for:

- Issuing Devices
- Monitoring testing activities
- Monitoring system activations
- Monitoring system trouble and coordinate repairs
- Training staff

- Entering Data
- Collection of issued equipment upon employee departure
- Other administrative functions

Departments shall follow facility-specific procedures and manufacturers' recommendations for use and service of equipment.

PAS Protocol

General PAS Setup

- Security Integrator**:**
  - Shall perform all necessary setup and programming of the PAS.
  - Any modification to the system shall be performed by the Security Integrator at the request of OMH.

User Access Levels

- Security Integrator:
  - Security Integrator technicians will have administrative access to perform all functions for each PAS and will have the exclusive ability to make any changes to passwords, permissions, and system setup.

- Chief Safety Officer, DFAS and Safety Officers: Each facility's CSO, DFAS and Safety Officers will have the following permissions:
  - Basic System Operation
  - Add Personnel and assign transmitters as directed
  - Remove Personnel from the system as directed
  - View Alarms
  - Silence Alarms
  - Reset the System
  - Run Reports

System Passwords

- Security Integrator will change the passwords for each PAS as requested by OMH.
- Passwords will be retained by the following (passwords will not be retained by, or available to, any facility staff other than CSO):
  - Security Integrator
  - CSO

CCTV System

The use of properly designed and installed closed circuit television (CCTV) technology is an effective method for recording, monitoring, and reviewing certain activity within the OMH Adult, Children's, Forensic and Secure Treatment and Rehabilitation Center (STARC) inpatient environments.

- Adult and Children's inpatient settings – the primary function of CCTV cameras is to provide video recording and video documentation of interactions between OMH staff and OMH clients. Camera installations are generally limited to areas where patients and staff would have interactions, such as day rooms, patient dining areas, patient corridors, elevators and elevator lobbies, and recreation spaces. Cameras are prohibited in staff-

only areas, bathrooms, bedrooms, and other areas that have a reasonable expectation of privacy.

- Forensic and STARC inpatient settings – CCTV cameras are authorized in all areas referenced in the Adult and Children's inpatient environments. Additionally, for Forensic and STARC settings, CCTV coverage/usage must be significantly expanded due to the higher level of security required in these environments. This includes active video surveillance and monitoring of the hospital's forensic perimeter, surveillance of truck traps, loading docks, building entrances and exits and other areas as approved by ASSG. Installation of audio recording devices, such as microphones, are the OMH standard for all CCTV cameras installed in patient-occupied spaces in the Forensic and STARC settings. Cameras and microphones are not approved for patient bedrooms, bathrooms, or staff offices.

Video recordings can be especially valuable as a reference for allegations of abuse and neglect, staff and client injuries, and other matters regarding employee administrative leave. **All facility requests to deviate from the CCTV camera standards referenced above must be expressively approved by the Director of ASSG**.

While meeting OMH and facility safety and security requirements, Video Surveillance systems must also conform to any HIPAA, consumer privacy, and legal regulations. Provisions must be made to prevent VSS monitors from being viewed by unauthorized personnel.

CCTV System Protocol

Preservation, Documentation, Storage and Chain of Custody of Recorded Video:

There will be instances necessitating the preservation of recorded video beyond the standard 30-day archive period. These situations include, but are not limited to, alleged criminal acts by clients and/or OMH personnel, staff misconduct, and/or policy violations.

Identified video recording must be preserved on OMH/ITS approved CD, DVD or encrypted password protected Flash Drive by personnel with the appropriate access level and title to perform this task. The decision on which medium to use will be determined by the size of the video recording.

Specific incidents can be "tagged" by the safety department or Risk department personnel on digital technology recording systems to eliminate the possibility of deleting or overriding the selected video clip.

- **Preservation of Video Recordings:**
  - Upon determination that recorded video requires preservation beyond the standard 30-day retention period, facility personnel with the appropriate access level and title shall locate the appropriate recorded video clips and save them to the Workstation hard drive.
  - Using OMH/ITS approved CD, DVD or encrypted/password protected Flash Drive, the video shall be burned CD/DVD or saved to the flash drive. The medium used shall be dependent upon the size of the recorded video clips. The video viewer must be saved, or burned, along with the recorded video.

- A review of the video on the CD/DVD or Flash drive shall be conducted to verify the integrity of the preserved video. Upon confirmation, the video clip shall be deleted from the workstation hard drive.
- Specific incidents can be “tagged” by the Safety Department or Risk Department personnel on digital technology recording systems to eliminate the possibility of deleting or overriding the selected video clip.

- **Documentation of Preserved Video Recording**
  - Video that is saved to Flash Drives or burned to CD/DVD is to be labeled with the following information:
    - Video Identification #
    - Beginning and Ending Time of the event.
    - Date of the Incident
    - Location of the Incident (Be Specific: Facility Name, Bldg. Name/Number, Floor, Unit Name/Number or Cottage Name/Number and specific location, e.g., TV room, Bedroom, Recreation Yard, etc.)
    - Name(s) of Staff Involved
    - Name(s) of Identified Witnesses
    - Name(s) of consumers Involved w/Case #

- **Storage of Preserved Video Recording:**
  - All preserved video shall be stored in a secure location with restricted access.
  - The location shall be determined by the facility’s Chief Safety Officer and approved by the facility Executive Director.
  - Storage time will be 7 years unless otherwise directed.

- **Chain of Custody**
  - There are circumstances in which preserved video will be requested, or subpoenaed, for use in disciplinary hearings, court proceedings or for review by other persons external to OMH. In these cases, the request is to be made and approved via established policy and procedure. Notification to the facility shall be made pursuant to those procedures.
  - Upon receipt of approval to make duplicate copies, the Facility Chief Safety Officer shall assign a Safety Officer with the appropriate access level to burn/copy the requisite number of CDs/DVDs or Flash Drives while always maintaining possession of the Master Copy.
  - Prior to transferring the media storage devices to the requesting party(s), the Chief Safety Officer, or designee, shall require the recipient to sign a formal document, prepared by the OMH Legal department that stipulates, minimally, to the following:
    - Video Identification Number
    - Date and Time of Transfer to the recipient
    - Name and Title of the recipient
    - Agency, department, or entity they represent
    - Method of Storage to ensure security and confidentiality of the video while in their possession.
    - Method of disposal and notification to OMH of same
    - HIPPA acknowledgement and compliance (Refer to OMH Policy and Procedure Manual for protocol)

- **General Network Video Recorder (NVR) Setup**
  - Security Integrator will setup each NVR for 30 days retention at 15 frames per second, 4 CIF or, digital megapixel equivalent.
  - No NVR will be setup for motion detection unless approved by the OMH and facility Security and Facility Risk staff. Each camera will be recorded continuously at 15 frames per second, 4 CIF, or digital megapixel equivalent.

- **User Access Levels**
  - **Security Integrator:** Security Integrator technicians will have administrative access to perform all functions for each DVR and NVR. Security Integrator technicians will have the exclusive ability to make any changes to passwords, permissions, and system setup.
  - **Chief Safety Officer and Facility DFAS:** Each facility's CSO and DFAS will have the following permissions:
    - View live video
    - View recorded video (no capability to delete recorded video)
    - Operate PTZ cameras
    - Download recorded video to external media
    - Download recorded video to View Station hard drive
    - Shut down the DVR or NVR in an emergency situation
  - **Safety Officer:** Each facility's Safety Officers will have the following permissions:
    - View live video
    - View recorded video (no capability to delete recorded video)
    - Operate PTZ cameras

  NOTE: Facility Risk members have been added to those who will be issued a review workstation and/or have access to recorded video for review and downloading.

- **Passwords**
  - Security Integrator will change the passwords for each DVR and NVR.
  - Passwords will be retained by the following (passwords will not be retained by, or available to, any facility staff):
    - Security Integrator
    - OMH Capital Operations
    - CSO

- **Additional Protocols**
  - Access to digital recordings and events on Remote View Stations shall be password protected under the direction of the Chief Safety Officer or designee.
  - Cameras shall be provided at all sally ports and employee entrances and all exterior exits to monitor and record activity
  - Cameras shall be provided in courtyards to record and monitor activity within fenced areas.
  - Cameras shall be provided in all elevator cabs. In Forensic settings only, microphones shall also be provided.
  - In Forensic Settings only, audio recording shall be provided in locations where clients congregate under the supervision of OMH staff, e.g., elevators, dining rooms, dayrooms and living unit hallways. Microphones, or provisions (cabling) for

microphones will be determined on a case-by-case basis by the facility administration in concert with ASSG/Central Office and Safety.
    - Recording shall not be permitted in bedrooms, bathrooms, and other areas where there is an expectation of privacy.
    - Safety Officers shall conduct daily reviews of the camera views to ensure all cameras are functioning and, conduct Monthly reviews of recorded video to make sure video is being recorded. And lastly, record both reviews on the designated forms.
    - Safety Officers are directly responsible for working to maintain security at OMH facilities. Safety Officers are expected to follow the appropriate protocol for camera system operation and to ensure that they, and others, abide by these protocols. Ongoing re-training must be provided to Safety Officers to cover new developments in the security equipment or procedures, and to refresh and reinforce understanding and use of the protocol.
    - Training must be provided as a standard part of the new employee Orientation process. On-going re-training must be provided to all safety, locksmith, and other staff to cover new developments and established protocols in the security equipment or procedures, to refresh and reinforce understanding and use of the Protocol.

ACCESS CONTROL TECHNOLOGY- LENEL Access System

The LENEL Access System is supported by central servers that connect to workstations at each facility.

All staff are directly responsible for maintaining security at OMH facilities and as such are expected to adhere to protocol for building access and make certain others abide by these protocols.

- All staff must use assigned access devices whenever entering or exiting an area so equipped.
- Psychiatric center locations that require the enhanced level of security provided by a combination of two or more access control authentications. These locations include, but are not limited to, Pharmacy, Medical Records, Cash Office, and OITS Rooms as approved by the facility.
    - All staff assigned to these areas must use this dual access control technology.
    - No other persons are to be given access without supervisor approval and documentation. This applies to all locations that require enhanced security and the use of Dual Technology Card readers, this is intended to prevent unauthorized employees from entering these special areas.
    - Keypad codes for dual technology readers shall be chosen during the ID card issuing process and stored by Safety in the access control database.

Lenel System Protocol

- **Employee and Consumer ID Badges**
    - The client's name on the card shall not be legible from more than three feet to protect the privacy of the consumer.
    - Employee departments and/or titles shall be included to identify the employee capacity and responsibility.

- Employee numbers will not be printed on the cards to reduce the possibility of lost or stolen ID numbers.
- All employees, contractors, and visitors shall be required to wear ID badges at all times while in the facility.
- All entering visitors will present their identification to security personnel at the outer lobby security window. Security personnel will notify the person to be visited or the staff member responsible for that visitor, requesting verification of the visitors' credentials and appointment. Upon suitable verification, security personnel will issue a temporary identification ID badge (or access/ID card) Failure to provide adequate credentials or to secure suitable verification will result in denial of entry. Visitors leaving the facility will follow a similar procedure, identifying themselves at the inner lobby security station and returning their temporary identification ID badge (or access/ID card). Visitors who have received temporary identification and are escorted by staff as authorized by the Chief Safety Officer, may access the facility at any staff entry during their visit but must always conclude their visit at the main entrance.
- All ID badges shall be marked for return to issuing facility if lost. Return address information is to be printed on the back side of the card.
- Where implemented by the facility, a temporary Visitor Management ID badge shall be issued at the safety post personnel with the visitor's picture and name. Supportive ID shall be provided by the visitor.

- **General Access Control System Setup**
  - **Security Integrator** shall perform all necessary data transfer/conversion (if required).
  - **Subsequent data entry** to be performed by trained authorized facility personnel.

- **User Access Levels**
  - **Security Integrator:** Security Integrator technicians will have administrative access to perform all functions for each Access Control system. Security Integrator technicians will have the exclusive ability to make any changes to passwords, permissions, and system setup.
  - **Chief Safety Officer, DFAS and Safety Officers:** Each Facility CSO, DFAS and designated Safety Officers will have one or more of the following permissions:
    - Basic System Operation
    - Add Personnel and assign access privileges as directed
    - Remove Personnel from the system as directed
    - View Alarms
    - Run Reports
    - Create Facility Specific I.D. cards

- **Passwords**
  - **Security Integrator** will change the passwords for each Access Control system as requested by OMH.
  - **Passwords** will be retained by the following (passwords will not be retained by, or available to, any facility staff):
    - Security Integrator
    - OMH Capital Operations