Olive View-UCLA MEDICAL CENTER

COUNTY OF LOS ANGELES
DEPARTMENT OF HEALTH SERVICES

Policy Title:	**FACILITY ACCESS CONTROLS**		
Category:	10 - Medication Management	**Policy No.:**	1011
Originally Issued:	5/14/2019	**Update (U)/Revised (R):**	5/14/2019
Distribution:	**Hospital-Wide** ☒	**If not Hospital-Wide, Other:**	

PURPOSE:

To define the process for ensuring County IT resources are protected by physical security measures that prevent tampering, damage, theft or unauthorized access

DEFINITION(S):

ACCESS: The ability or the means necessary to read, write, modify or communicate data/information or otherwise make use of any system resource.

INFORMATION TECHNOLOGY (IT): A term that encompasses all forms of technology used to create, store, exchange, and use information in its various forms (business data, personal health information, voice conversations, still images, motion pictures, multimedia presentations, and other forms, including those not yet conceived).

SAFEGUARDS: Administrative, Physical and Technical actions or measures, and policies and procedures to protect Protected Health Information (PHI) and Personally Identifiable Information (PII).

For a more complete definition of terms used in this policy and/or procedures, see Department of Health Services (DHS) Policy Number 935.00 - “Information Technology and Security Policy”.

Olive View-UCLA Medical Center access control must include the following components to ensure the Confidentiality, Integrity and Availability of data:

Contingency Operations:

Olive View-UCLA Medical Center must be responsible for developing, testing, implementing and maintaining the Information Technology (IT) Contingency Operations Plan that provides access when necessary to restore Information Systems and/or lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

Olive View-UCLA Medical Center Security Plan:

Olive View-UCLA Medical Center must be responsible for developing, testing, implementing and maintaining the IT component of the Security Plan to safeguard computer information assets therein from unauthorized physical access, tampering, and theft.

Physical Access Control and Validation (DHS Workforce Members and Visitors):

Olive View-UCLA Medical Center must be responsible for developing, testing, implementing and maintaining the IT component of the Access Control and Validation Procedure to control and validate each person's access IT resources based on his/her role or function, including visitor control, and control of access to software programs for testing and revision.

Olive View-UCLA Medical Center must be responsible for developing, testing, implementing, and maintaining a Security Maintenance Record to document repairs and modifications to the physical components as they relate to security (e.g., hardware, walls, doors, locks, etc.)

POLICY:

Olive View-UCLA Medical Center must implement policies and procedures to limit physical access to electronic information systems in which they are housed, while ensuring that properly authorized access is allowed. These policies and procedures must be consistent with the Department of Health Services Policy No. 361.23 - "Safeguards for Protected Health Information (PHI)".

PROCEDURE:

Contingency Operation

Identify systems and data and their location that, if lost, will be reestablished and/or restored as a part of the Olive View-UCLA Medical Center disaster recovery plan or emergency mode of operation plan.

Identify the workforce members that need Olive View-UCLA Medical Center and/or system access in the event of a disaster or emergency.

Create and implement a backup authentication scheme to regulate Olive View-UCLA Medical Center access in the event of a disaster or emergency. Since electronic means cannot be relied upon during an emergency, a "manual" authentication scheme should also be developed.

When determining these access means, emergency communications means must be considered to ensure authorized access is granted in the event an obstacle is encountered.

The contingent access scheme must be tested periodically to ensure operational functionality.

These procedures must be coordinated with other components including the "Olive View-UCLA Medical Center Information Technology (IT) Contingency Plan".

Olive View-UCLA Medical Center Security Plan

The Olive View-UCLA Medical Center Security Plan is intended to limit physical access to Olive View-UCLA Medical Center's electronic information systems and the areas in which they are housed. It is also intended to allow physical access to electronic information systems and the areas in which they are housed, to workforce members who need access in furtherance of County business.

To accomplish this purpose, Olive View-UCLA Medical Center is taking a "layered approach". This means that access measures will be "layered" – the more sensitive the area or system, the more restrictive the access control.

Exterior of Premises

Olive View-UCLA Medical Center Security Plan must:

Clearly define the security perimeter of the premises and buildings.

Ensure that the perimeter defined above is physically sound (i.e., no gaps in which a break-in is relatively easy).

Ensure that all external doors are adequately secured against unauthorized access by installing locks, alarms, or other access control devices.

Ensure that sensitive areas are monitored as necessary (e.g., video surveillance cameras with video recording capabilities).

Provide for a reception area (staffed at least during business hours in which visitors may access the building through a single entrance to the area).

Define the instances in which visitors are allowed, including areas they visit and escort requirements.

Ensure that any fire doors on the security perimeter are alarmed, have a self-closing mechanism, and are compliant with fire regulations.

If any of the measures above are determined to be unfeasible, the Plan must provide justification and must ensure the security of the premises through other means.

Interior of Premises

Olive View-UCLA Medical Center Security Plan must:

Ensure that any necessary physical barriers are extended from real floor to real ceiling.

Ensure that all doors to interior areas requiring compartmentalization or added security are adequately protected against unauthorized access by installing locks, alarms, or other access control devices.

Ensure that sensitive areas are monitored as necessary (e.g., video surveillance cameras with video recording capabilities).

Ensure that all doors and windows lock by default and that adequate security measures are in place for windows at ground level.

Intrusion detection systems are included where appropriate to provide additional security to interior premises and buildings.

Ensure that vacant secure areas are locked and periodically inspected.

- If any of the measures above are determined to be unfeasible, the Plan must provide a justification and must ensure the security of the premises through other means.

Olive View-UCLA Medical Center Equipment

Olive View-UCLA Medical Center Security Plan must:

Ensure that any Olive View-UCLA Medical Center equipment requiring additional levels of protection be isolated from other equipment to the extent possible.

Position workstations such that monitor screens and keyboards are not directly visible to unauthorized persons.

Provide controls to guard against equipment theft (e.g., closed-circuit television monitoring devices, alarms, locks, and controlled access).

Provide controls to guard against fire damage (e.g., smoke detectors, fire alarms and fire extinguishers as reasonable to protect the electronic information system.)

Provide control to guard against water damage (e.g., elevating workstations and other equipment, as reasonable to protect the electronic information).

Provide controls to ensure air quality is maintained, that is appropriate for the equipment (e.g., air conditioning, heating, dust filters, and air dehumidifiers/humidifiers, as reasonable to protect the electronic information system.

Provide controls to guard against damage caused by vibrations or electrical supply interference.

Provide controls to guard against power surges and outages, such as multiple power feeds, backup generators, and uninterruptible power supplies.

Ensure OVMC IT and System Owners are working together as a team from inception to completion of each system implementation. Once the system is in production, all system maintenance aspects (version upgrades, routine maintenance, security patches, etc.) and any other performance related issues shall be managed as a team. The system server(s) shall be located at the Data Center with the appropriate access controls. Any exceptions to this policy will require both approval by the Chief Information Officer (CIO) and the OVMC Information Security Office (DISO) and appropriate procedures to safeguard both the system *and* the data. OVMC IT and System Owners must properly document the process for handling version upgrades, routine maintenance, security patches and must institute controls for incident reporting and response.

- If any of the measures above are determined to be unfeasible, the Plan must provide a justification and must ensure the security of the information through other means.

Access Control and Validation

The Olive View-UCLA Medical Center CIO/designee must ensure that the System Manager/Owners:

Configure access controls to allow workforce members access based on the least privilege rule.

Include a means to update the Olive View-UCLA Medical Center access control settings to reflect workforce member status changes.

Ensure that visitors sign in upon entering the Olive View-UCLA Medical Center Information System areas if working as an outside contractor.

Ensure that visitors are escorted by appropriate personnel where required by Olive View-UCLA Medical Center Security Plan.

Ensure that workforce members testing and/or revising software programs are identified, authenticated and authorized to perform those activities.

Maintenance Records

The Olive View-UCLA Medical Center CIO/designee must:

Identify the physical components of the Olive View-UCLA Medical Center that are relevant to IT security (e.g., hardware, walls, electronic systems, doors and locks).

Approve and oversee any IT security-related physical modifications to Olive View-UCLA Medical Center.

Create a maintenance record or log and ensure that it is updated for each such modification.

Ensure proper chain-of-custody for pertinent items like keys, smart badges and access codes.

ATTACHMENTS/FORMS:

None

REFERENCE(S)/AUTHORITY:

- 45 Code of Federal Regulations (CFR), Part 164, Subpart C, Section 164.310(a)(1) and (a)(2)(i-iv)
- Board of Supervisors Policy No. 6.106, Physical Security
- DHS Policy No. 935.10, Physical Access Control and Validation

APPROVED BY:

Susan Aintablian (Chief Information Officer)