OLIVE VIEW-UCLA MEDICAL CENTER
POLICY & PROCEDURE

NUMBER: 1404
VERSION: 1

SUBJECT/TITLE: **PERSON OR ENTITY AUTHENTICATION**

POLICY: Olive View-UCLA Medical Center Facility CIO/designee must establish and document facility-based procedures for each of the following requirements and submit such procedures for approval to the DISO or designee.

1. A user authentication mechanism (e.g., unique user identification and password, biometric input, or a user identification smart card) must be used for all workforce members seeking access to any network, system, or application that contains PHI and other confidential information.

2. Two-factor authentication, in which the user provides two means of identification, one of which is typically physical (e.g., a secure ID card using a one-time code), and the other of which is typically something memorized (e.g., a secret Personal Identification Number (PIN)) is required for all systems receiving a Risk Analysis Sensitivity score of "HIGH" and for all remote access.

Workforce members seeking access to any network, system, or application must not misrepresent themselves by using another person's User ID and Password, smart card, or other authentication information.

Users are not permitted to allow other persons or entities to use their unique User ID and password, smart card, or other authentication information.

Olive View-UCLA Medical Center CIO's/designees must ensure that the Olive View-UCLA Medical Center System Managers/Owners implement the system authentication mechanism that is appropriate for the risk expected for the system. System Managers/Owners must document the selected system authentication mechanism in the System Security Documentation of Olive View-UCLA Medical Center policy, "System Access Control" that accompanies the electronic data system.

PURPOSE: To verify that a person or entity seeking access to Protected Health Information (PHI) and other confidential information is the one claimed.

DEPARTMENTS: All

DEFINITIONS: Authentication: means validation of the identity of the user.

For a complete definition of terms used in this policy/procedure, see the Olive View-UCLA Medical Center Information Security Glossary, Attachment I to Olive View-UCLA Medical Center policy "Information Technology and Security Policy".

PROCEDURE:

AUTHORITY: 45 Code of Federal Regulations, Part 164, Subpart C, Section 164.312(d)
Board of Supervisors Policy Nos:
6.100, Information Technology and Security Policy
6.101, Use of County Information Technology Resources

References: Olive View-UCLA Medical Center Policies: Safeguard for Protected Health Information (PHI) Security Management Process: Risk Management Workforce Security Information Access Management System Access Control Acceptable Use Policy for County Information Technology Resources	
Approved by: VEC-2010 April	Date: 05/03/2010
Review Date: **05/28/2022**	Revision Date:
Distribution: Information Systems, Olive View Hospital-Wide Policies	
Original Date: 05/03/2010	