SANTA CLARA VALLEY HEALTH & HOSPITAL SYSTEM

Administrative Policies and Procedures **HHS #512.2**

Central Services Policies and Procedures

April 22, 2015

TO: SCVHHS Executive Leadership Group

FROM: René G. Santiago
Director, SCVHHS

SUBJECT: **Information Systems Access and Confidentiality**

REFERENCE:
HHS# 512.5 Electronic Email
HHS# 585.17 Safeguarding Protected Health Information
HHS# 585.2 Workforce General Obligations Regarding Uses & Disclosures of Protected Health Information
HHS# 585.7 HIPAA Privacy Workforce Training
County IT Security Policy 3.0 General Security Policy
County IT Security Policy 4.0 Local User Logon and Authentication

POLICY:

Santa Clara Valley Health and Hospital System (SCVHHS) protects the confidentiality of patient and employee data in its information systems. Only authorized staff who have been trained and completed required documentation will be allowed access to such information systems. Unauthorized access or violation of SCVHHS security policies and procedures may result in disciplinary action up to, and including, termination of employment.

Access to information systems which contain protected health information (PHI) and employee data is restricted through the use of unique logon I.D., strong passwords, physical location of terminals, computers, end-user devices, or other methods. Individual logon I.D. and password must be assigned to users to access SCVHHS computer systems. Said passwords will be used as their legal hand-written signature. The password will be changed periodically. The logon I.D. and password will be disabled/deleted upon termination of employment.

PROCEDURE:

Responsible Party	**Action**
Department Manager/Designee	Ensure their staff has signed the appropriate User Responsibility Statement before their user accounts has been created. Provides appropriate User training, including the SCVHHS policies and procedures on confidentiality, privacy and access to PHI.

Department Manager/Designee

Promptly submits a System Access Termination Form to the SCVHHS Information Services (IS) Service Desk when a User has been terminated or is transferred to another County Agency.

As part of out-processing procedures, ensures that terminating User access to SCVHHS computer systems has been properly removed.

Provides IS with a monthly report of contractors, volunteers and temporary employees that have been terminated.

Information Services

Ensure strong password policies have been applied in order to access SCVHHS computer systems.

When notified of User termination that their logon I.D. has been disabled.

Ensure the "logon banner" has been applied and displays at time of logon.

SCVHHS employee or workforce member

Shall comply with applicable SCVHHS policies and procedures related to the privacy and security of PHI and other confidential information maintained in electronic or other formats.

Shall understand that they are held responsible for all activities that occur within their assigned users account(s).

Human Resources

Promptly notifies IS when a User has been terminated.

As part of out-processing procedures, ensures that terminating User access to SCVHHS computer systems has been properly removed.

Provides IS with a monthly report of contractors, volunteers and temporary employees that have been terminated.

Issued: 03/01/1993
Revised: 04/22/2015