ADMINISTRATIVE POLICY AND PROCEDURE

Subject: COMPUTER WORKSTATION USE AND SECURITY **Policy No.:** A331

Supersedes:	November 26, 2019	Review Date:	February 8, 2023
Origin Date:	May 1, 2007	Revision Date:	February 8, 2023

PURPOSE:
To restrict workstation use and access to Protected Health Information (PHI) and other confidential information by using Physical, Administrative, and Technical security controls.

POLICY:
Rancho Los Amigos National Rehabilitation Center (RLANRC) must ensure workstation security procedures are enforced on all County-owned computing devices, including but not limited to desktop computers, laptops, mobile devices, cellphones, printers, and fax machines provided for County business.

1. All users must use computing devices commensurate with the sensitivity of the information accessed from the workstations.

2. All users must take reasonable physical security precautions to prevent unauthorized physical access to sensitive information from workstations. These precautions include considering the physical attributes of the surroundings (e.g., concealing video displays and securing unattended workstations).

3. RLANRC System Managers/Owners must implement physical safeguards to permit only authorized users' access to workstations with accessibility to confidential and sensitive information.

   All Users who use workstations, as described above, must be trained to exercise proper security practices. Training and documentation must be in accordance with DHS Policy No. 361.1, DHS Privacy and Security Compliance Program policies and procedures, including RLANRC Administrative Policy No. 334, Privacy and Security Awareness and Training Policy, and RLANRC Administrative Policy A300, Computer Security and Protected Health Information (PHI) Guidelines.

DEFINITIONS:
Protected Health Information (PHI) means Individually identifiable health information (45 CFR 160.103) held or transmitted by DHS or its business associate(s) in any form or medium, whether electronic, paper, or oral, relating to the past, present or future physical or mental health condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual. The information identifies the individual or, with respect to which there is a reasonable basis to believe, can be used to identify the individual. (45 CFR 160.103)

Workforce Member means Employees, business associates, contracted employees, consultants, volunteers, other County departments, and/or individuals whose conduct in the performance of work for DHS, its offices, programs, or facilities is under the direct control of the Department, office, program, or facility regardless of whether the person is paid or unpaid.

Revised: 6/09, 11/19, 2/23
Reviewed: 6/09, 11/19, 2/23

Approved By: Aries Limbaga

Digitally signed by
Aries Limbaga
Date: 2023.03.21
15:43:22 -07'00'

For a complete definition of terms used in this policy and procedure, see the DHS Information Security Glossary, Attachment I to DHS Policy No. 935.00, DHS Information Technology and Security Policy, available on the Rancho Intranet site under "Resources/HIPAA" and at the DHS Intranet site https://intranet.ladhs.org/isb/securitypoliciesprocedures.htm.

PROCEDURES:

RLANRC CIO/designee must ensure that the following workstation security procedures are implemented within Rancho Los Amigos National Rehabilitation Center. Workstations are all County-owned computers, including but not limited to mobile devices such as laptops, tablet PCs, cellphones, printers, and fax machines used for County business.

I. Workstation Use

These procedures are intended to include documented instructions delineating the proper functions to be performed by RLANRC workforce members and how those functions are to be performed (e.g., logging off before leaving a workstation unattended) to maximize the security of health information.

Access and Use of Workstation and Network Services Measures to limit unauthorized access must include the following:

A. Configuration of workstations and network services.

a. RLANRC System Managers/Owners must configure workstations and network services to allow only authorized access to the workstation and network services (e.g., data, applications, intranet, and Internet).

b. Workforce members must have the authorization to access a workstation and the appropriate rights to do so. Users must not access confidential or sensitive information from a workstation unless they have the authorization and such access is necessary to do their job.

B. Permitting authorized access to workstations and network services through the use of controls. RLANRC CIO/designee is responsible for creating, designing, and implementing measures to limit unauthorized access by workforce members to workstations and network services.

a. Unique User IDs and Passwords

1. The Department of Human Resources is responsible for assigning a unique user ID to each workforce member to identify and track the individual's identity when logging into workstations, networks, or applications.

2. Workforce members must protect their passwords. They must not write down their passwords and place them at or near the workstation (e.g., a note taped to the monitor or placed under the keyboard).

3. Logging into workstations, networks, or applications with another workforce member's user's identification or password is prohibited.

4. Users must not share their unique user identification (login/system identifier).

5. All user's passwords must be changed every ninety (90) days.

6. Passwords must be at least eight (8) characters and, ideally, contain a combination of alpha and numeric characters if the system allows it.

7. Multi-Factor Authentication (MFA) is highly recommended and requires the user to provide two means of identification, one of which is typically a physical authenticator (e.g., a one-time password code or biometric recognition). The other, which is usually something memorized (e.g., password), must be used as recommended in the Facility Master Security Management Report. (Refer to DHS Policy No. 935.01, Security Management Process: Risk Management). Some Rancho Los Amigos laboratory devices may not support MFA but are configured with compensating security controls.

8. Other User Authentication Methods
   With authorization from the DHS Departmental Information Security Officer (DISO), RLANRC CIO may utilize other User authentication methods (e.g., badge readers, biometric devices, tokens).

C. Access to Workstations Not in Use

a. Workstations not in use must be password protected and locked.

b. Workstations must be set up to generate a password-protected screen saver when the computer receives no input for a specified period (20 minutes of inactivity on the keyboard or mouse, based on the risk assessment result). Other “lockout” schemes that protect against unauthorized access to confidential or sensitive information may be approved by the RLANRC CIO/designee.

D. Workstations must display an appropriate warning banner before gaining operating system access when technologically feasible.

II. Access and Use of Mobile Computers and Storage Devices

A. Mobile devices must be pre-approved and registered for use at RLANRC by the facility CIO/designee. These devices must be managed and controlled through auditable inventory logs.

B. Workforce members must exercise good judgment in determining the amount of necessary data stored on their mobile devices to perform their functions.

C. Access to mobile devices must be protected at all times, consistent with the procedures outlined in the Access and Use of Workstation and Network Services section above and RLANRC Administrative Policy A300.2, Portable Computer Security Guidelines.

D. Mobile devices containing sensitive information (e.g., confidential patient information) must be encrypted. Refer to Administrative Policy A300, Computer Security, and Protected Health Information (PHI) Guidelines.

E. A workforce member must not leave mobile devices unattended in non-secure areas when traveling.

F. Mobile devices left in cars must be stored out of sight, and the vehicle must be locked.

III. Data Security and Physical Attributes of Surroundings

Workforce members must be aware of the physical attributes of the workstation's surroundings. Precautions must be taken to prevent unauthorized access to unattended workstations by auto-locking the workstation and auto-activating a screensaver after 20 minutes of inactivity. To limit the ability of an unauthorized individual to access or remove confidential or sensitive data from a workstation, the following measures must be taken:

A. Confidential data (e.g., patient information) must be password protected, encrypted, or stored on a secure network.

B. Confidential and HIPAA-protected health information must be encrypted when stored on a portable computer.

C. Confidential data must not be downloaded without authorization from the RLANRC CIO/designee.

D. Confidential data must not be saved on removable devices (e.g., external hard drives, USB drives, or third-party email or cloud storage providers) without proper encryption safeguards and authorization from the RLANRC CIO/designee.

E. Removable media containing confidential data (e.g., patient information) must be stored in secured areas and encrypted. Some Rancho Los Amigos audio recorders and cameras are not encrypted but use compensating security controls to secure the data.

F. Printers should not be left unattended in non-secure areas when printing confidential or sensitive information.

G. Disposal of confidential electronic records stored on removable or external media (e.g., hard drives or USB drives) must be in accordance with DHS Policy No. 935.13, Device and Media Controls.

H. Use caution when viewing and entering confidential information.

I. The work area layout and design must shield the workstation screen's view from the public unless the requirements of subsection III.J, below, apply and are complied with.

J. Where it is not possible, through layout and design of the work area, to shield the workstation screen from view, devices like privacy screens and shields are to be used.

IV. Workstation Security

These procedures are intended to put physical safeguards to restrict access to information through securing RLANRC workstations.

A. General

a. Workstations in public or open areas must be physically secured in a locked room, locked cabinets, or firmly anchored to deter unauthorized movement. Security cameras or additional forms of monitoring should be considered in high-risk areas.

b. Mobile devices must be secured when not in use. These devices must either be carried on persons or stored in secured areas.

c. Workstation equipment must not be removed from the premises unless documented and pre-approved by the user’s supervisor.

d. Devices must be located per the equipment manufacturer’s operational specifications.

e. Inventory and maintenance records must be maintained for all workstations.

f. Computer monitors must be positioned away from common areas, or a privacy screen must be installed to prevent unauthorized access or observation, as referenced in DHS Policy No. 361.23, Safeguards for Protected Health Information (PHI).

B. Hardware/Software

a. Workforce members must not change the system configuration of their workstation without proper authorization (e.g., network configuration).

b. Workforce members must not install or uninstall software on their workstations without proper authorization and licensing (e.g., downloaded Internet software, games, patches, plug-ins, screen savers).

c. Only authorized users may install/uninstall software and perform repair services on workstations.

d. Workforce members-must not re-enable USB ports or unauthorized peripherals on workstations with access to confidential data unless the workforce member is authorized to use those drives.

e. RLANRC CIO/ designee is responsible for ensuring the appropriate controls are in place when transporting equipment off premises for maintenance (i.e., maintenance contract must include business associate language).

f. All hardware and software connected to an RLANRC's network services must be managed centrally within each RLANRC.

AUTHORITY:
Code 45 of Federal Regulations, Part 164, Subpart C, Section 164.310(a) (2) (iv) (b) and (c)
Board of Supervisors Policies:
6.100, Information Technology and Security Policy
6.101, Use of County Information Technology
6.102, Countywide Antivirus Security Policy
6.106, Physical Security
6.107, Information Technology Risk Assessment

CROSS-REFERENCES:
DHS Policies:
361.8, "Minimum Necessary Requirements for Use and Disclosure of Protected Health Information (PHI)."
361.23, Safeguards for Protected Health Information (PHI)
935.01, Security Management Process: Risk Management
935.03, Workforce Security
935.06, "Security Incident Report and Response."
935.11 "(Computer) Workstation Use and Security
935.13, Device and Media Controls
DHS Policy No. 935.14, System Access Control
935.20, DHS Acceptable Use Policy for County Information Technology Resources

RLANRC Policies:
Admin Policy A260, Confidentiality of Social Security Numbers

Admin Policy A300, Computer Security and Protected Health Information (PHI) Guidelines
Admin Policy A300.1, Electronic Mail (E-Mail) and Acknowledgement
Admin Policy A300.2, Portable Computer Security Guidelines
Admin Policy A332, Privacy, and Security Awareness and Training
IMS Policy 324.5, Prevent, Detect, Report, and Removal of Malicious Software