ADMINISTRATIVE POLICY AND PROCEDURE

Subject: WORKFORCE SECURITY **Policy No.:** A333

Supersedes:	December 3, 2015	Review Date:	March 21, 2023
Origin Date:	May 1, 2007	Revision Date:	March 21, 2023

PURPOSE:
To ensure Rancho Los Amigos National Rehabilitation Center (RLANRC) workforce members have appropriate access to data systems and information contained in data systems and to prevent unauthorized access to confidential and Protected Health Information (PHI).

POLICY:
This policy ensures the security (confidentiality, integrity, and availability) of PHI and other sensitive information. RLANRC will develop and implement security procedures that protect the confidentiality of PHI and additional sensitive information. Access will be granted based on the workforce member's need to know and job responsibility.

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, to concerning which there is a reasonable basis to believe, can be used to, and determine the individual. (45 CFR 160.103)

Workforce Members means Employees, business associates, contracted employees, consultants, volunteers, other County departments, and 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.

PROCEDURES:
RLANRC Departmental Information Security Officer must work with facility System Managers/Owners and Human Resources to develop and coordinate the implementation of the workforce security procedures.

I. RLANRC Workforce Authorization and Supervision Procedure

RLANRC facility System Managers/Owners must ensure that workforce members are granted proper access authorization by the Information Management Services department Policy 904, Information Access Management.

The Authorization and supervision process must consist of the following components:

1. RLANRC facility managers/supervisors must identify and supervise workforce members who work with or have access to PHI and other confidential information. RLANRC facility

managers/supervisors must identify the minimum information necessary for workforce members to perform their job.

2. RLANRC facility System Managers/Owners or designees must identify the security levels necessary for securing the system and allow workforce members to perform their jobs. RLANRC facility System Managers/Owners will assign access to workforce members with the appropriate security level needed to perform their job functions.

3. RLANRC facility managers/supervisors must restrict access to PHI and other confidential information to unauthorized workforce members.

4. RLANRC facility managers/supervisors must provide authorization and supervision to workforce members and others who need to be in areas where PHI and other confidential information may be accessed and take appropriate safeguards to ensure those who may be exposed to PHI and additional sensitive data are made aware of the policies protecting that information.

II. RLANRC Workforce Clearance Procedure

RLANRC facility System Managers/Owners must ensure that workforce members' access to PHI and other sensitive data is limited to the minimum necessary to perform their job responsibilities.

The clearance process must consist of the following components:

1. RLANRC Human Resources (HR) or designee must implement proper workforce clearance procedures. Refer to DHS Policy No. 703.1, Criminal Records Background Check/Fingerprinting Policy.

2. RLANRC Human Resources (HR) or designee must ensure proper HIPAA training has been provided to all new and transferred workforce members from other county departments. Refer to Rancho Administrative Policy No. 334, Privacy and Security Awareness and Training.

3. RLANRC Human Resources (HR) or designee must ensure that each new workforce member receives and signs the County Acceptable Use Policy for Information Technology Resources agreement and an acknowledgment of DHS Policy No. 935.20 during the new hire orientation and that each workforce member completes the Computer Security and Protected Health Information acknowledgment during the annual Performance Evaluation process. The signed acknowledgments will be filed in the workforce member's official personnel folder. Those policies define their responsibility for protecting the confidentiality, integrity, and availability of all RLANRC information resources and restrictions for utilizing those resources.

4. RLANRC System Managers/Owners or designees must ensure all applications for access to a data system are complete and approved by the appropriate workforce managers/supervisors.

III. RLANRC Workforce Termination Procedure (Access)

RLANRC Human Resources and facility System Managers/Owners must ensure that departing workforce members' access to all PHI and other confidential information is terminated upon employment termination or transfer from RLANRC.

The termination process must consist of the following components:

1. RLANRC facility System Managers/Owners must be notified by the workforce member's supervisor, by RLANRC HR department's/designee, or by the Information Management Services (IMS)

department's designee assigned to monitor and acknowledge employee status changes in the County-Wide Payroll System or Active Directory, as follows:

a. As soon as possible, but in no circumstance later than the day the workforce member's employment or another service arrangement with RLANRC ends.

b. As soon as possible, when a workforce member's status/function/responsibility has changed.

2. Supervisors of workforce members who have been involuntarily terminated must contact the Enterprise Help Desk at (323) 409-8000 as soon as possible but no later than the close of the same business day or the end of the workforce member's work shift.

3. RLANRC must terminate the workforce member's access to PHI or other confidential information upon notification by the workforce member's supervisor, by the RLANRC HR department's designee, or by the Information Management Services (IMS) department's designee assigned to monitor and acknowledge employee status changes in the County-Wide Payroll System or Active Directory, when the workforce member terminates employment (voluntarily or involuntarily) or transfers to another facility or County department.

   Access termination must be as follows:
   a. As soon as possible but in no circumstance later than five business days when the end of employment is voluntary.

   b. As soon as possible but in no circumstance later than close of the same business day or end of a workforce member's work shift when the end of employment is involuntary.

4. RLANRC facility System Managers/Owners must promptly review the workforce member's access to PHI and other confidential information and modify the member's access as needed.

AUTHORITY:
45 Code of Federal Regulations, Part 164, Subpart C, Section 164.308 (a) (3) (ii)
Board of Supervisors Policy Nos.:
6.100, Information Technology and Security Policy
6.101, Use of County Information Technology Resources

CROSS REFERENCES:
DHS Policies:
361.8, Minimum Necessary Requirements for Use and Disclosure of Protected Health Information (PHI)
703.1, Criminal Records Background Check/Fingerprinting Policy
935.03, Workforce Security
935.20, Acceptable Use Policy for County Information Technology Resources

Rancho Policies:
Admin Policy A254, Termination Transfer
Admin Policy A300, Computer, 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 A331, Computer Workstation Use, and Security
IMS Policy 324.5, Prevent, Detect, Report, and Removal of Malicious Software
IMS Policy 904, Information Access Management