RANCHO LOS AMIGOS NATIONAL REHABILITATION CENTER

ADMINISTRATIVE POLICY AND PROCEDURE

Subject: COMPUTER SECURITY AND PROTECTED HEALTH INFORMATION (PHI) GUIDELINES **Policy No.:** A300

Supersedes:	December 3, 2015	Review Date:	February 8, 2023
Origin Date:	January 1, 1982	Revision Date:	February 8, 2023

PURPOSE:
This policy and procedure aims to ensure the security and proper use of data, software, and electronic equipment within Rancho Los Amigos National Rehabilitation Center (RLANRC). To ensure Rancho (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:
It is the policy of RLANRC to ensure the security (confidentiality, integrity, and availability) of PHI and other confidential 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 job responsibility and on a "Need to know" basis.

Each workforce member (defined as full or part-time, temporary or permanent employees, contractors, students, agency personnel, registry, volunteers, interns, or others) is individually responsible for the protection of County data and information processing resources to which they have access due to employment at RLANRC.

PROCEDURES:
Each RLANRC employee shall acknowledge and abide by this policy.

A. PHYSICAL SECURITY

1. **Locking Devices:** Locking devices will be installed, wherever feasible, on all County-owned workstations and laptops.. This will be done when the equipment is delivered or as necessary.

2. **Removal of Computers, Laptops, Printers, and other Hardware:** County-owned computers, laptops, and printers may only be removed from the premises with the permission of the Chief Executive Officer (CEO), on the recommendation of Information Management Services (IMS). IMS must be notified in writing and in advance of any required movement of computer equipment outside the premises. All laptops and removable media devices (e.g., external hard drives, flash drives, etc.) containing PHI must be encrypted.

3. **Relocation of Computers, Laptops, Printers, and other Hardware:** IMS personnel will handle the internal movement of computer hardware only unless other arrangements have been coordinated with local law enforcement and IMS. Requests for movement of computer hardware will consist of a services request submitted by the requesting department with adequate lead time.

(Laptop users refer to Policy A300.2 Portable Computer Security Guidelines and Portable Computer Security Guidelines Agreement.)

B. SOFTWARE

RLANRC licenses the use of computer software from a variety of vendors. The software developer usually copyrights such software. RLANRC has no authority to make copies of the software except for backup or archival purposes unless expressly authorized.

1. **Policy:** It is the policy of RLANRC to respect all computer software copyrights and to adhere to the terms of all software licenses to which RLANRC is a party. The Chief Information Officer (CIO)/designee serves as RLANRC's Software Manager and is responsible for enforcing these guidelines. RLANRC employees may not duplicate any licensed software or related documentation for use on RLANRC premises or elsewhere unless RLANRC has been authorized to do so by agreement with the licensor. Unauthorized software duplication may subject workforce members to discharge from County service and RLANRC to civil and criminal penalties under the United States Copyright Act.

   Workforce members may not give the software to any outsiders, including clients, contractors, customers, or other individuals unless formal approval is received from IMS. RLANRC workforce members may only use RLANRC-owned software per the applicable license agreement.

2. **Approval to Purchase Software/Applications:** The requestor must obtain permission and acknowledgment from IMS and Administration to purchase the software. The requestor is required to provide the following information when purchasing software or applications not included in the standard applications utilized by RLANRC (a list of approved applications is available from IMS):

   a. **Need:** The requesting department must establish that applications currently licensed and supported by RLANRC will not meet their specific requirements. The requestor should be able to provide evidence in the form of a functional comparison between requested software and those applications supported by IMS.

   b. **Justification:** The requesting department must establish a rationale for the requested software. The explanation should address such areas as cost-benefit, an enhancement to providing patient care, satisfying regulatory requirements, etc.

   c. **Equipment:** The requesting department must prove that all necessary or special hardware is or will be in place to support any software acquisitions. This would include network requirements, workstations, special monitors, peripherals, and hardware requirements.

   d. **Documentation:** The requesting department will be responsible for acquiring and maintaining any documentation necessary to manage the software. This would include user and necessary technical manuals.

   e. **Training:** The requesting department will be responsible for securing necessary training for those individuals responsible for managing the application and, in some cases, the systems on which the application is installed.

f. **Staffing:** Requesting department will identify those individuals who will manage the software (i.e., data input, file maintenance, report generation, IMS interface, etc.). Staffing must be adequate to assure successful implementation.

g. **Maintenance:** The requesting department must ensure that the requested software is supported and that is routinely updated with the vendor's provided fixes, patches, and updates.

h. **Security:** The requesting department will be responsible for providing and demonstrating that adequate security precautions will be implemented to ensure that confidential patient and employee information is not compromised.

3. **Budgeting for Software:** The requesting department's responsibility will be to budget for software training and ongoing maintenance/support when acquiring computer software programs.

4. **Software Maintenance and Control:** It will be the responsibility of the requesting department to ensure that adequate steps are taken to provide for long-term management (e.g., hardware/software license upgrades, system maintenance, and contract renewal), hardware requirements, documentation, and training when acquiring proprietary software programs.

5. **Acquisition of Software.** All software acquired by RLANRC must be purchased through the proper procurement process. Any software purchased outside the usual procurement process such as personal funds, grants, or other funding should be reviewed with IMS Department before installation. The software installed without IMS knowledge may not be supported by RLANRC and will be immediately reported to the Department Head or Service Chief, CIO/designee, and CEO.

6. **Registration of Software:** When software is delivered, it must first be delivered to the software manager or designee to complete registration and inventory requirements. The software manager is responsible for seeing that registration cards are completed and returned to the software publisher. Software must be registered in the name of RLANRC and the department in which it will be used. Because of personnel turnover, software should never be registered in the name of an individual user. IMS will maintain a register of all RLANRC software and will keep a library of software licenses. The registration must contain:

   a. Name, date, and source of software acquisition
   b. Location of such installation
   c. The inventory control number of the hardware on which each copy of the software is installed
   d. The name of the department
   e. The software product serial number

7. **Installation of Software:** After the above registration requirements have been met, the software will be installed by IMS. When available, manuals, tutorials, and other valuable materials will be provided to the user. Once installed on the hard drive, the original will be kept in a safe storage area maintained by IMS.

8. **PC System Configuration/System Setup:** Computer systems shall be set up and configured by IMS Technicians only. PCs are configured to work with attached equipment and should not be altered, e.g., desktop configuration, printer settings, etc. Modifications to system configuration are prohibited by workforce members other than IMS technical staff.

9. **Offsite Computers:** RLANRC/County-owned computers are County assets and must be utilize virus-free software. Only software purchased through the above procedures may be used on RLANRC computers. Employees are not permitted to bring software from home to install on RLANRC computers. Employees using County owned computers at home, e.g., notebook computers, are not permitted to load any software in addition to the applications installed by the manufacturer and/or IMS.

10. **Application Development:** Software applications developed for the County are the sole property of the County. These applications may be created by County workforce members and contracted consultants. Unless otherwise dictated by licensing agreements, these applications belong to the County. Deleting, modifying, or removing these applications from the premises must be approved by the Department Head or Service Chief and IMS. Any deliberate employee actions to alter or delete such applications, to the detriment of RLANRC, may result in discipline up to and including discharge from County service.

11. **Shareware:** Shareware is copyrighted software distributed freely through the internet and online systems. Downloading executable files must be cleared with IMS (see Internet Use, section B4 (Policy no. A239). It is the policy of RLANRC to pay shareware authors the fee they request to use of their products. Registration of shareware products will be handled the same way as commercial software products.

12. **Periodic Audits:** IMS will conduct routine software audits of County owned machines to ensure that RLANRC complies with all software licensing agreements. IMS will search for computer viruses during the audits and eliminate any found. Employees are expected to adhere to the audit process. Discrepancies or violations of software licensing agreements, copyright laws, or the detection of unauthorized software will be immediately reported to the Department Head or Service Chief, CIO/designee, and CEO.

C. SYSTEM ACCESS

The System Access Request (SAR) form, signed by the manager, will be used to identify user access for various systems. Refer to the “Cross References” section on page 8 for System Access procedures for multiple systems.

D. DATA SECURITY

Users of data shall protect County data as required by the data owner. Confidential information maintained on computer systems will be handled as outlined in Confidentiality of Records (Policy no. B503) and Patient Access to Health Records (Policy no. B503.1).

1. **Backup Procedures:** Backups should be encrypted and password protected to prevent unauthorized access, End-users should establish procedures for backing up their data regularly. Backups are to be stored away from the computer in a secure area. Staff is encouraged to backup their data to the Local Area Network (LAN); IMS policies and procedures encourage users to back up regularly to avoid data loss should the hard drive fail or become unusable.

2. **System Log-off:** Workstations shall not be left unattended when logged on to a system. Workforce members shall log off the system when leaving the workstation for any reason to prevent inadvertent or deliberate disclosure of confidential information or unauthorized modification to the data.

3. **Output Protection:** The output of data from such systems is also considered confidential. Output can be in the form of reports, miscellaneous information, etc. The output from such systems will be stored in a secure area to protect the confidentiality of data and will only be provided to those needing to know. Sensitive and confidential reports will be appropriately labeled as confidential.

4. **Removal:** Confidential or sensitive information in electronic form must be encrypted and confidential paper documents must be transported in lockboxes.
5. **Portable Computers and Storage Devices**: All mobile computers and storage devices must be encrypted. Workforce members should contact the Enterprise Help Desk at (323) 409-8000 for encryption instructions or requests. Laptop users refer to Policy A300.2 Portable Computer Security Guidelines and Portable Computer Security Guidelines and Acknowledgment.

6. **Protected Health Information (PHI):** To comply with DHS Policy 935.03, Workforce Security, RLANRC information system managers must ensure the following components are met:

    a. RLANRC managers/supervisors must identify workforce members who work with or have access to PHI and other confidential information. RLANRC facility managers/supervisors must determine the minimum information access required by these workforce members to do their job.
    b. RLANRC System Managers/Owners or designees must identify the security levels necessary for the system's security and allow workforce members to perform their jobs. RLANRC System Managers/Owners will assign workforce members to the minimum security level needed to perform their job functions.
    c. RLANRC managers/supervisors must restrict access to PHI and other confidential information by unauthorized workforce members.
    d. RLANRC 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.

E. **USER ID AND PASSWORD**

Passwords must always be protected and are considered confidential. Passwords should be created to ensure that only you can access systems. Failure to adhere to the following rules may result in discipline, including discharge from County service.

1. **Password Confidentiality:** Workforce members should never share passwords. Passwords should not be written down anywhere, including but not limited to keyboards, tabletops, post-notes, etc. Passwords should never be verbally shared with others.

2. **Password Changes:** Passwords will be renewed every 90 days to limit the unauthorized use of a compromised password.

3. **Password Integrity:** Workforce members should never create predictable passwords.

4. **User Responsibility:** Individuals issued a password are responsible for using that password, including any misuse.

5. **Password Distribution:** Department of Human Resources controls issuing of usernames for access to County systems and applications. The workforce member's supervisor must request entry in writing, with approval from an authorized Department Head, Service Chief, or their designee.

6. **Resetting Passwords:** Workforce members can reset their password by contacting the Enterprise Help Desk via email or phone. They can also reset their passwords using the online password reset portal.

7. **Authorization Levels:** Access to County computer data and associated processing privileges shall be granted only as required to perform the tasks and responsibilities currently assigned to an individual or an operating unit. Individuals with custodial access to data owned by another department shall protect the data as required by the data owner.

F. **GENERAL CONTROLS**

1. **Computer Connectivity:** Computers connected to the County's host systems must comply with all Internal Service Department (ISD) and Information Technology Services (ITS) security requirements applicable to computer-based methods such as user identification and passwords. Questions regarding these requirements may be directed to IMS.

2. **Personal Use:** Personal computers can be used for Teleworking purposes if the proper network security and identity safeguards are in place, such as Virtual Desktop Infrastructure (VDI), Multi-factor Authentication, or approved mobile applications),

G. USE OF ELECTRONIC MAIL (E-mail)

See Electronic Mail, Policy A300.1.

H. CONSEQUENCE OF SECURITY VIOLATION

Any workforce member violating the above security policies, including procedures specific to a particular system, may have their access privilege revoked and be subject to discipline up to and including discharge from County service.

Questions regarding data security or the proper use of equipment should be directed to the appropriate area manager or Departmental Information Security Officer.

I. MALICIOUS SOFTWARE AND INFORMATION SECURITY BREACHES

All employees, volunteers, contractors, and other persons who process, store, and transmit data at Rancho Los Amigos are informed on how to prevent, detect, remove, and report malicious computer software, such as computer viruses and information security breaches.

1. When malicious software or any virus is detected on a computer system, do not shut off the computer and do not use the machine until IMS technical staff have investigated and resolved the problem.

2. Write down all the error messages and relay this information to the Departmental Information Security Officer or Enterprise Help Desk.

3. If users suspect their system has been compromised, they should immediately contact the Enterprise Help Desk at (323) 409-8000.

J. VIRUS SCANNING OF ALL SOFTWARE AND IMPORTED DATA

All software and data imported onto computers through physical (e.g., thumb drives) or (e.g., e-mail or downloaded from the internet) can be scanned for viruses before the file is opened and read by the user. Contact the Enterprise Help Desk at (323) 409-8000 if assistance is needed.

REFERENCES:

Department of Health Services, County of Los Angeles,
Data Security Policy and Use of Electronic Equipment, No. 935, Effective May 2000.
Internet Use, No. A329, Effective May 2000.
Confidentiality of Records, No. B503, Effective January 1982
Patient Access to Health Records, No. B503.1, Effective February 1994
County Fiscal Manual

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)
361.24, Privacy and Security Awareness and Training
935.06, Security Incident Report and Response
935.11, (Computer) Workstation Use and Security
935.13, Device and Media Control
935.14, System Access Control
935.20, Acceptable Use Policy for County Information and Technology Resources

Rancho Policies:
Admin Policy A254, Termination, and Transfer
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
Admin Policy A332, Privacy and Security Awareness and Training
IMS Policy 324.5, Prevent, Detect, Report, and Removal of Malicious Software
IMS Policy 501, HIS System Access
IMS Policy 510, Access to the Internet
IMS Policy 511, Access to GroupWise, E-Mail
IMS Policy 521, WebRx System Access
IMS Policy 521, Addendum (How To Procedure) for WebRx System Access
IMS Policy 609, Access to the Hospital Information System (Affinity) Data at Other County Hospitals
IMS Policy 610, Rancho User Access to the Hospital Information System (Affinity) Data at Other County Hospitals
IMS Policy 904, Information Access Management

Medical Imaging Policy Policy pending for Fuji PACS Synapse System Access

Rehabilitation Therapy Rehab Therapy Policy RT 307, RTIS Access

Rancho Los Amigos National Rehabilitation Center

Computer Security and Protected Health Information Guidelines (A300) and Electronic Mail (A300.1)

I understand it is the policy of Rancho Los Amigos National Rehabilitation Center (RLANRC) that all personnel (defined as employees, contractors, students, agency personnel, volunteers, whether they are permanent, temporary, part-time, or other) are personally responsible for the protection of all RLANRC information, HIPAA-related protected health information, data, and information processing resources which they have access to by virtue of employment by RLANRC.

I hereby acknowledge being responsible for the proper use of electronic equipment and the privacy, integrity and availability of RLANRC data in compliance with RLANRC Computer Security and Protected Health Information (PHI) Guidelines Policy (A300) and Electronic Mail (A300.1).

ACKNOWLEDGMENT

By signing where indicated below, I acknowledge and affirm each of the following:

1. I have received and carefully reviewed a copy of RLANRC Computer Security and Protected Health Information (PHI) Guidelines Policy (A300) and Electronic Mail Policy (A300.1).

2. I understand that I shall be held personally responsible and accountable for complying with these policies.

3. I am aware that if I violate any provisions of these policies, I will be subject to disciplinary action that may include discharge from service, and/or agency.

_____ _____

EMPLOYEE NAME (PRINT) EMPLOYEE NO.

_____ _____

SIGNATURE DATE

_____

SUPERVISOR'S NAME (PRINT)

_____ _____

SUPERVISOR'S SIGNATURE DATE

Distribution: Original - Employee Official Personnel Folder, Copy - Employee, Copy - Departmental Area File