SUBJECT: PRIVACY AND SECURITY AWARENESS AND TRAINING POLICY

Policy No.: A332
Supersedes: June 1, 2009
Revision Date: December 3, 2015

PURPOSE: To outline the Privacy and Security training for Rancho Los Amigos National Rehabilitation Center (RLANRC).

POLICY: Health information is personal and sensitive information that is accorded special protection under federal and state law. It is the policy of the Department of Health Services (DHS) to ensure all members of its workforce are trained on their responsibilities related to protecting the confidentiality, integrity and availability of Protected Health Information (PHI) and other confidential information. Each time a material change is instituted in the Privacy and Security policies or procedures, DHS' facilities will train each member of its workforce whose functions are affected by the change.

DEFINITION: Protected Health Information (PHI) means individually identifiable information relating to the past, present or future physical or mental health condition of an individual, provision of health care to an individual, or the past, present or future payment for health care provided to an individual.

Workforce or Workforce Members means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the Department, its offices, programs or facilities, is under the direct control of the Department, office, program or facility, regardless of whether the entity pays them.

PROCEDURE: I. WORKFORCE TRAINING REQUIREMENTS

A. The privacy and security training must provide workforce members with information on how to handle PHI and other confidential information in accordance with DHS' privacy-related and security-related policies.

1. HIPAA Awareness Training (Privacy and Security): General privacy and security training for all RLANRC workforce members who have limited or no access to PHI and other confidential information in the course of their work.

APPROVED BY:

Signature(s) on File.

2. HIPAA Comprehensive Training: Role-based privacy training designed for clinical and specialty staff who have access to PHI and other confidential information or provide direct patient care (e.g., physicians, nurses, ancillary services, and health information management staff). Security training required for all staff responsible for PHI and other confidential information.

3. HIPAA Security Specialized Training: Role-based security training required for facility CIOs, System Managers/Owners, System Administrators and IT staff responsible for implementing and maintaining administrative, physical and technical security safeguards.

4. HIPAA for Business Associates: Required for the segment of RLANRC employees who provide contract and purchase order procurements.

5. The facility Chief information Officer or Departmental Information Security Officer may include additional security awareness training topics aimed at reducing the risk of improper access, use, and disclosure of confidential and/or sensitive information, taking into consideration the information from the System Description Report and the Risk Analysis and Management of each computer system on campus.

B. All members of RLANRC's workforce will receive privacy and security training within 60 days of new employment or transfer into the facility.

1. Training during new employee orientation to address general components for workforce privacy and security compliance. This training includes HIPAA awareness and information all RLANRC employees must know related to security and the access, use, and handling of PHI and other confidential information. Training content must include, as a minimum, the following topics:

   a. Training on guarding against, detecting and reporting malicious software.
   b. Rules for creating, changing and safeguarding passwords.
   c. Login training including the importance of monitoring login attempts and reporting discrepancies. Systems will provide previous login information after each successful login.
   d. Periodic security reminders through automated means, login banners, pamphlets, broadcast e-mails, etc.
   e. Training on workstation usage and related safeguards. Refer to DHS Policy No. 361.23, Safeguards for Protected Health Information (PHI).
   f. Security incident reporting.
   g. Training on media control covering removal and receipt of hardware/software including access control, accountability, data backup, data storage, mobile storage devices and disposal of electronic data.

h. Training on acceptable use of County information technology resources. Refer to DHS Policy No. 935.20, Acceptable Use Policy For County Information Technology Resources.

2. Training during facility orientation on all policies and procedures regarding PHI privacy and security as they relate to the facility.

3. Job specific orientation to educate employees on confidentiality and to address PHI privacy and the security functions necessary for job performance.

C. Thereafter, training for new members of RLANRC's workforce will include Administrative Policy A300- Computer Security and Protected Health Information Guidelines and Agreement, revised May 2007 or later. It shall be read and acknowledged as part of the annual Performance Evaluation process.

D. For all members of its workforce whose job responsibilities change because of new or changed policies or procedures, RLANRC will update training within 30 days after the effective date of the change

E. If an existing employee's job functions change due to a position change within DHS, training on health information privacy and security will be conducted during orientation at the employee's new position, or within the first 30 days after the employee's first work day in the new position, (See Section II-"Training Related to Updates or Changes in Policies and Procedures" below.)

II. TRAINING RELATED TO UPDATES OR CHANGES IN POLICIES AND/OR PROCEDURES

Training related to updates or changes in policies and procedures will be executed through workforce training, facility training, or job specific training. Updates and changes will be incorporated into the training materials used for new employee, facility, and job specific orientation.

This training will be an ongoing, evolving process in response to environmental and operational changes affecting the security of electronic information and as RLANRC's security needs and procedures change. The amount and timing of security awareness training will be left to the discretion of the facility but not less than once every two years.

III. TRAINING DOCUMENTATION REQUIREMENTS

A. Health Services Administration, Compliance Division will maintain documentation in electronic or written format on all training provided to members of the DHS workforce.

B. Documentation of training will consist of date, time, workforce trainee name and type of training session attended.

C. Training documentation will be placed in workforce personnel file and/or tracked in a County, DHS, or RLANRC training database.

D. This documentation will be retained for six years from the date of its creation or the date when it was last in effect, whichever is later.

If, however, a DHS/RLANRC entity is subject to a longer documentation retention period as a part of a regulatory, compliance and/or accreditation requirement [e.g. Medicare, Medicaid, JCAHO] then the documentation mentioned above must be retained for the longer period.

E. Training will consist of:

- At New Employee Orientation or departmental training, the employee completes HIPAA Comprehensive Self-Study Guide.
- An employee reads and takes the quiz. Answer sheet on page 35 is placed in HR file.
- At New Employee Orientation or departmental training, the employee is given DHS Policy 935.20 (DHS Acceptable Use Policy for County Information Technology Resources).
- An employee reads and signs the 3-page agreement form and the acknowledgment form to 935.20, which are placed in HR file.
- At New Employee Orientation or departmental training, employee is given DHS Policy 361.23 (Safeguards for Protected Health Information (PHI)
- An employee reads and signs the acknowledgment, which is placed in HR file.

AUTHORITY: 45 Code of Federal Regulations Parts 160 and 164, Section 164.530(b), "Administrative Requirements- Training", Section 164.530(j), "Standard: Documentation."

Board of Supervisors Policies:

6.101, Use of County Information Technology
6.102, Countywide Antivirus Security Policy

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
935.03, Workforce Security
935.06, Security Incident Report and Response
935.11, Workstation Use and Security
935.13, Device and Media Controls
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 A331, Computer Workstation Use and Security
IMS Policy 324.5, Prevent, Detect, Report, and Removal of Malicious Software