Los Angeles County Department of Health Services

Policy & Procedure Title:	Privacy and Security Awareness and Training Policy		
Category:	300-399 Operation Policy	**Policy No.:**	361.24
Originally Issued:	04/14/2003	**Update (U)/Revised (R):**	03/01/2017 (R)
DHS Division/Unit of Origin:	Patient Safety, Risk Management, Privacy, & Compliance		
Policy Contact – Employee Name, Title and DHS Division: Jennifer Papp, R.D., DHS Privacy Officer, Privacy Compliance			
Contact Phone Number(s):	(213) 240-8283		
Distribution: DHS-wide ☒	**If not DHS-wide, other distribution:**		

PURPOSE:

The purpose of this policy is to outline the Privacy and Security training for the Department of Health Services (DHS).

DEFINITION(S):

Protected Health Information (PHI) means individually identifiable information relating to 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, contract staff, affiliates, volunteers, trainees, students, and other persons whose conduct, in the performance of work for DHS, is under its direct control, whether or not they receive compensation from the County.

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 receive general education and specialized training as necessary and appropriate for the workforce member to carry out their job functions within the DHS 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. It is mandatory that all workforce members participate in privacy- and security-related training as specified in this policy.

Privacy and security awareness training must be completed prior to gaining access to PHI.

PROCEDURE:

I. PRIVACY AND SECURITY TRAINING

The privacy and security training must provide workforce members with information on their responsibilities related to security and access, use, and handling of PHI and other confidential information in accordance with DHS' privacy- and security-related policies.

A. Awareness Training. General HIPAA/privacy and security training for all DHS workforce members during on-boarding as a new hire, transfer, or student.

B. Awareness Training will be provided during the on-boarding process and/or new workforce member orientation, and ongoing through various methods including handbooks, e-mail blasts, newsletters, etc. Awareness training during the on-boarding process will include a review of DHS privacy- and security-related policies and procedures. Awareness training will be provided annually through the use of facility orientation/reorientation handbook.

Prior to gaining access to PHI, workforce members must complete Awareness Training, which consists of the workforce member's signed acknowledgment of receipt of the following documents.

1. DHS' Notice of Privacy Practices
2. DHS Policy 361.8, Minimum Necessary Requirements for Use and Disclosure of Protected Health Information (PHI)
3. DHS Policy Number 361.10, Disciplinary Actions for Failure to Comply with Privacy Policies and Procedures
4. DHS Policy 361.111, Reporting Privacy and Security Related Breaches
5. DHS Policy Number 361.23, Safeguards of Protected Health Information (PHI)
6. DHS Policy 935.20, Acceptable Use of County Information Technology Resources
7. DHS Disciplinary Manual and Guidelines

C. Comprehensive Training: Training for new members of DHS' workforce will address workforce privacy and security compliance. This training provides the workforce with information on the policies and procedures with respect to PHI and what DHS' workforce must know in order to perform their job. This training must be completed within 30 days from the date of hire/assignment, but not later than 60 days.

D. On-going Security Awareness Training Content: Awareness training methods can include e-mail messages, discussions during staff meetings, screen savers, log-in

banners, newsletter/internet articles, posters, etc. DHS security awareness training shall include, as a minimum, the following topics:

1. Training on guarding against, detecting, and reporting malicious software.

2. Rules for creating, changing, and safeguarding passwords.

3. Login training including the importance of monitoring login attempts and reporting discrepancies. Systems will provide previous login information after each successful login.

4. Periodic security reminders through automated means, login banners, pamphlets, broadcast e-mails, etc.

5. Training of workstation usage and related safeguards. Refer to DHS Policy No. 361.23, Safeguards for Protected Health Information (PHI).

6. Security incident reporting.

7. 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.

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

   Each Facility CIO/designee shall, as appropriate, include additional security awareness training topics aimed at reducing the risk of improper access, use, and disclosure of confidential and/or sensitive information.

E. Thereafter, training for new members of DHS' workforce will include:

1. All employees will completed privacy and security awareness training during on-boarding or new employee orientation to address general components for workforce privacy and security compliance. Comprehensive privacy and security training must be completed within 30 days from date of hire/assignment, but not later than 60 days

2. Job specific orientation to educate employees on confidentiality and to address PHI privacy and the security functions necessary for job performance. Managers/supervisors are responsible for providing this training when the workforce member arrives at the worksite.

3. For all members of its workforce whose job responsibilities are affected by new or changed policies or procedures, DHS will train the identified workforce

within a reasonable period of time after the material change becomes effective.

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

A. The DHS Privacy Officer/designee will assure that the content of the Privacy and Security Awareness and Training programs is updated, as appropriate, to reflect any material changes in the DHS/County privacy- and security-related policies and procedures.

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

C. This training will be an ongoing, evolving process in response to environmental and operational changes affecting the security of electronic information and as DHS' security needs and procedures change.

III. TRAINING DOCUMENTATION REQUIREMENTS

A. Each DHS facility will maintain documentation in electronic or written format on all HIPAA/privacy and security related training provided to members of its workforce.

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

C. Each workforce member will be required to attest that they have received training on HIPAA and acknowledgement of duties and responsibilities. Training documentation will be placed in workforce personnel file and/or tracked in an electronic database.

D. Documentation of each workforce member's successful completion of training and any updated training must be retained for a minimum of six years from the date of the training.

REFERENCE(S)/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
6.111 Information Security Awareness Training