COUNTY OF LOS ANGELES DEPARTMENT OF HEALTH SERVICES

HARBOR-UCLA MEDICAL CENTER

SUBJECT: PRIVACY AND SECURITY AWARENESS AND TRAINING POLICY **POLICY NO. 701**

PURPOSE:
To outline the Privacy and Security training for Harbor-UCLA Medical Center.

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

DEFINITIONS
Protected Health Information (PHI): 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 Members: 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 they are paid by the entity.

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 Harbor-UCLA Medical Center's privacy-related and security-related policies.

1. HIPAA Awareness Training (Privacy and Security): General privacy and security training for all Harbor-UCLA Medical Center Workforce members who have limited or no access to PHI and other confidential information in the course of their work.
2. HIPAA Comprehensive Training: Role-based privacy training designed for clinical and specialty staff who have access to PHI and other confidential

EFFECTIVE DATE: 04/14/03 **SUPERSEDES**
REVISED: 01/05, 08/14
REVIEWED: 1/05, 11/12, 08/14, 08/17
REVIEWED COMMITTEE: N/A

APPROVED BY:

Kim McKenzie, RN, MSN, CPHQ
Chief Executive Officer

Anish Mahajan, MD
Chief Medical Officer

Patricia Soltero Sanchez, RN, BSN, MAOM
Chief Nursing Officer

Signature(s) on File.

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 Harbor-UCLA Medical Center employees who provide contract and purchase order procurements.
5. Security Training Content: Harbor-UCLA Medical Center security awareness training 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, date 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.

   Harbor-UCLA Medical Center's CIO 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, taking into consideration the information from the System Description Report and the Risk Analysis Report as specified in DHS Policy No. 935.01, Security Management Process: Risk Management.

B. All members of Harbor-UCLA Medical Center's workforce will receive privacy training no later than April 14, 2003 and security training no later than April 20, 2005.

C. Thereafter, training for new members of Harbor-UCLA Medical Center's workforce will include:
   1. Training during new employee orientation to address general components for workforce privacy and security compliance. This training includes HIPAA awareness and information, all Harbor-UCLA Medical Center employees must know related to security and the access, use, and handling of PHI and other confidential information.

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.

D. For all members of its workforce whose job responsibilities change because of new or changed policies or procedures, Harbor-UCLA Medical Center 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 Harbor-UCLA Medical Center, 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, whichever is sooner. (See Section II - "Training Related to Updates or Changes in Policies" 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 Harbor-UCLA Medical Center'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 REQUIREMENT

A. Harbor-UCLA Medical Center will maintain documentation in electronic or written format on all training provided to members of its 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 Harbor-UCLA Medical Center's 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, Harbor-UCLA Medical Center 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.

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