



**LOS ANGELES COUNTY DEPARTMENT OF HEALTH SERVICES
HARBOR-UCLA MEDICAL CENTER**

SUBJECT: PRIVACY AND SECURITY COMPLIANCE PROGRAM

POLICY NO. 701A

CATEGORY: HIPAA-Privacy and Security	EFFECTIVE DATE: 1/05
POLICY CONTACT: Keisha Belmaster	UPDATE/REVISION DATE:
REVIEWED BY COMMITTEE(S):	

PURPOSE:

To define the Privacy and Security Compliance Program for Harbor-UCLA Medical Center.

POLICY:

Harbor-UCLA Medical Center's administrative requirements for the Privacy and Security Compliance Program consists of twelve sections:

- I. **Privacy, Security and Confidentiality Training**
- II. **Disciplinary Actions for Failure to Follow Applicable Privacy and Security Policies**
- III. **Safeguards for Confidential and Protected Health Information**
- IV. **Disclosure of Protected Health Information (PHI) by Whistleblowers**
- V. **Workforce Member Crime Victims**
- VI. **Mitigation**
- VII. **Non-Retaliation**
- VIII. **Waiver of Individual Rights**
- IX. **Complaints Related to Harbor-UCLA Medical Center Privacy and Security Practices**
- X. **Personnel Designations**
- XI. **Implementing Changes to Privacy and Security Related Policies**
- XII. **Documentation of Privacy and Security Policies and Procedures**

I. Privacy, Security and Confidentiality Training


To ensure that Harbor-UCLA Medical Center workforce members understand their role and responsibility in protecting patient privacy, the facility provides Privacy and Security Program training to all workforce members. The training provided is tailored to meet the member's need to access protected information to perform assigned job duties or functions and consists of:

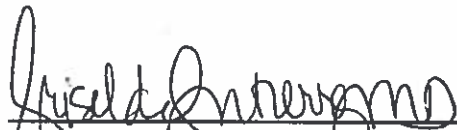
- A. An initial training of all current Harbor-UCLA Medical Center's workforce members at or near the time the privacy regulation becomes effective,

REVISED: 1/05, 2/22

REVIEWED: 1/05, 12/08, 6/12, 5/14, 7/17, 2/22

APPROVED BY:


 Anish Mahajan, MD
 Chief Executive Officer
 Chief Medical Officer


 Griselda Gutierrez, MD
 Associate Chief Medical Officer


 Jason Black, MBA, DNP, RN
 Chief Nursing Officer



LOS ANGELES COUNTY DEPARTMENT OF HEALTH SERVICES
HARBOR-UCLA MEDICAL CENTER

SUBJECT: PRIVACY AND SECURITY COMPLIANCE PROGRAM

POLICY NO. 701A

- B. Training of new workforce members within a reasonable time period following the member's addition to the workforce,
 - C. Retraining of workforce members whose job duties are affected by a material change in policy and/or procedure, and
- Training will be documented and maintained in either electronic or written format for each workforce member for six years.

II. Disciplinary Actions for Failure to Follow Applicable Privacy and Security Policies

- A. Harbor-UCLA Medical Center has policies and procedures regarding disciplinary actions that are communicated to all workforce members, agents, and contractors. Examples of possible sanctions or disciplinary actions include, but are not limited to, verbal warnings, notices of disciplinary action placed in personnel files, removal of system privileges, termination of employment, and sanctions or penalties imposed pursuant to contract. Workforce members, agents, and contractors are also advised that there may be civil or criminal penalties for misuse or misappropriation of protected health information (PHI) or for breach of security. Violations may result in notification to law enforcement, regulatory, accreditation, and licensure organizations.
- B. If there is reason to believe a member of the workforce has failed to follow the privacy policies, security protocols, or breached patient confidentiality, then an investigation will be initiated and documented. If the allegation is substantiated through the investigation, appropriate sanctions or discipline will be applied.
- C. Harbor-UCLA Medical Center will maintain documentation related to sanctions/disciplinary action of its workforce in either electronic or written format. This documentation will be retained in the workforce member's personnel record or other appropriate location depending on the category of the workforce member involved. This process will be imposed equitably throughout Harbor-UCLA Medical Center. Sanctions or discipline will be applied commensurate with the severity, frequency, and intent of the violation or breach.

III. Safeguards for Confidential and Protected Health Information

Safeguards are the administrative, technical, and physical protective measures and controls Harbor-UCLA Medical Center imposes to protect the privacy and security of PHI and confidential information.

These safeguards include but are not limited to: hardware and software security features, operating procedures, accountability procedures, access and distribution controls, management constraints, personnel security, and physical structures, areas, and devices. Safeguards for Protected Health Information are described in DHS Policy 361.23. A full treatment of security controls for protecting all confidential electronic data is documented in the suite of security policies DHS Policy 935.00 through 935.20.

- A. **Administrative Safeguards:** Harbor-UCLA Medical Center develops and maintains written policies, procedures, and technical processes that assure appropriate administrative safeguards to protect the privacy of PHI and the security of confidential information as follows:
 - 1. Security Management Process
 - 2. Assigned Security Responsibility
 - 3. Workforce Security
 - 4. Information Access Management
 - 5. Security Awareness Training



LOS ANGELES COUNTY DEPARTMENT OF HEALTH SERVICES
HARBOR-UCLA MEDICAL CENTER

SUBJECT: PRIVACY AND SECURITY COMPLIANCE PROGRAM

POLICY NO. 701A

6. Security Incident Procedures
7. Contingency Plan
8. Evaluation
9. Business Associate Contracts or Other Arrangements

B. Physical Safeguards: These safeguards provide reasonable protection of PHI from intentional or unintentional use. Physical safeguards address the following policies and procedures:

1. Facility Access Controls
2. Workstation Use
3. Workstation Security
4. Device and Media Controls

C. Technical Safeguards: Technical Safeguards address the need to protect, control and monitor access to electronic data. These safeguards include policies and procedures that address the following:

1. Access Control
2. Audit Controls
3. Integrity
4. Person or Entity Authorization
5. Transmission Security

D. Harbor-UCLA Medical Center is responsible for creating, implementing, and maintaining a risk management plan for both electronic and non-electronic information assets.

E. Verification of the development of safeguards is a responsibility of Harbor-UCLA Medical Center Privacy and Security Officers who may consult with Harbor's Privacy Manager, Security Information Officer, and/or other knowledgeable individuals.

IV. Disclosures of Protected Health Information (PHI) by whistleblowers

Harbor-UCLA Medical Center does not violate the privacy regulations if a member of the facility's workforce discloses PHI to a health oversight agency, public health authority authorized to investigate, health care accreditation organization, or to an attorney retained by a workforce member if the purpose of the disclosure is to report an allegation of unlawful conduct by Harbor-UCLA Medical Center, a violation of professional or clinical standards, or conditions that endanger patients.

V. Workforce Member Crime Victims

Harbor-UCLA Medical Center does not violate the privacy and security regulations if a member of its workforce, who is a victim of a crime, discloses PHI about the suspected perpetrator to a law enforcement official and the information disclosed is limited to the following information:

- Name and address,
- Date and place of birth,
- Social security number,
- ABO blood type and RH factor,
- Type of injury,
- Date/time of treatment,
- Date/time of death (if applicable), and
- Distinguishing physical characteristics (e.g., weight., height. gender, race, hair/eye color, facial hair, scars/tattoos)



**LOS ANGELES COUNTY DEPARTMENT OF HEALTH SERVICES
HARBOR-UCLA MEDICAL CENTER**

SUBJECT: PRIVACY AND SECURITY COMPLIANCE PROGRAM

POLICY NO. 701A

VI. Mitigation

To the extent practicable, Harbor-UCLA Medical Center will mitigate any known harmful effect from the use or disclosure of PHI that was in violation of the facility's security or privacy policies and procedures.

VII. Non-Retaliation

Harbor-UCLA Medical Center will not intimidate, threaten, coerce, or retaliate against persons for filing complaints; for testifying, assisting or participating in investigations, assisting or participating in compliance reviews, assisting or participating in proceedings or hearings under Part C of Title XI of the Social Security Act; or for opposing real or perceived unlawful acts or practices under this act provided the opposition is reasonable.

VIII. Waiver of Individual Rights

Harbor-UCLA Medical Center does not require an individual to waive his/her right to file a complaint or other rights with regard to their PHI as a condition for the provision of treatment or payment or employment.

IX. Complaints Related to Department of Health Services Privacy and Security Practices

- A. Harbor-UCLA Medical Center provides a process for filing a complaint or grievance regarding privacy practices.
- B. All complaints or grievances are investigated and documented. This documentation includes outlining the facts of the complaint or grievance, the investigative procedures and outcomes, and final resolution. Harbor-UCLA Medical Center maintains in either electronic or written format, documentation related to the filing of a complaint by an individual. This documentation will be retained for six years from the date of its creation or the date when it last was in effect, whichever is later.

X. Personnel Designations

- A. DHS has designated a Privacy Officer who is responsible for the development and implementation of the policies and procedures of the entity.
- B. Harbor-UCLA Medical Center has designated a Privacy Manager and a Security Information Officer who are responsible for working with the DHS Privacy and Security Officer in the implementation of the policies and procedures.
- C. Harbor-UCLA Medical Center has designated a contact person or office that is responsible for receiving complaints and is able to provide further information about matters covered by the Notice of Privacy Practices.

XI. Implementing Changes to Privacy and Security Related Policies

Harbor-UCLA Medical Center policies and procedures concerning PHI are implemented, revised, or changed as necessary or required due to changes in the law, health care practice, or entity situation. Policy or procedures that do not materially affect the content of the Notice of Privacy Practices are not changed unless the policy or procedural revisions are necessary to comply with the privacy regulations or the policy or procedure is documented prior to the effective date of the change. Implementing



LOS ANGELES COUNTY DEPARTMENT OF HEALTH SERVICES
HARBOR-UCLA MEDICAL CENTER

SUBJECT: PRIVACY AND SECURITY COMPLIANCE PROGRAM

POLICY NO. 701A

changes to security policies and Procedures are described in DHS Policy 935.19, Data Security Documentation Requirement.

- A. Necessary revisions or changes in policies, procedures, or the Notice of Privacy Practices (Notice) are documented and implemented in a timely manner. When applicable, affected groups receive notification of the changes:
 - 1) Policy and procedural implementation relative to a Notice are not made prior to the effective date of the Notice.
 - 2) Harbor-UCLA Medical Center reserves the right to make changes to the Notice needed to comply with revised state and/or federal privacy regulations or changes in Harbor-UCLA Medical Center's privacy and security policies.
 - 3) Changes of this type relate only to PHI received or created after the effective date of the Notice and are implemented after that effective date.
- B. Policies and procedures will be maintained in written or electronic format and retained for six years from the date of its creation or the date when it last was in effect, whichever is later.

XII. Documentation of Privacy and Security Policies and Procedures

Harbor-UCLA Medical Center documents and maintains in a written or electronic format all policies, procedures, and communications relating to the privacy practices for six years from the date of creation or the last date it was in effect, whichever is the longest. Documentation of security policies and procedures is described in DHS Policy 935.19, Data Security Documentation Requirement.

Harbor-UCLA Medical Center administrative department heads/managers, physician department chairs or unit medical directors and others as appropriate are responsible for the development, potential review and revision of the policies and procedures, and communications for their respective area(s). The period between reviews will not exceed three years.

All policies and procedures that affect Harbor-UCLA Medical Center should be approved in accordance with the facility's policy and procedure approval process.

REFERENCES

1. Code of Federal Regulations 45, Part 160 and 164; Section 164.530 "Administrative Requirements".
2. Code of Federal Regulations 45, Part 160 and 164; Section 164.502 "General Rules".
3. DHS Policy No. 361.2 Notice of Privacy Practices
4. DHS Policy No. 361.10 Disciplinary Actions for Failure to Comply with Privacy Policies and Procedures
5. DHS Policy No. 361.23 Safeguards for Protected Health Information
6. DHS Policy No. 361.12 Waiver of Rights
7. DHS Policy No. 361.13 Non-Retaliation
8. DHS Policy No. 361.22 Implementing Changes to Privacy-Related Policies
9. DHS Policy No. 361.24 Privacy and Confidentiality Training
10. DHS Policy No. 361.26 Mitigation
11. DHS Policy Nos. 935.00 – 935.20 pertaining to information technology security measures.

