

**LOS ANGELES COUNTY  
DEPARTMENT OF HEALTH SERVICES  
HARBOR-UCLA MEDICAL CENTER AND COASTAL CLUSTER HEALTH CENTERS**

**HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)  
SECURITY RULE  
COMPREHENSIVE SELF-STUDY GUIDE**

Content adapted from: *Health Care Compliance Strategies, Inc. and  
The DHS HIPAA Security Rule Comprehensive Self-Study Guide*

**CONTRIBUTING EDITORS**  
**Harbor-UCLA Medical Center HIPAA Security Team**

***Gail V. Anderson, M.D.***  
Medical Director

***Peter Allen***  
Building Crafts Manager  
Mechanical Services

***Angela Brown***  
Assistant Administrator  
Hospital Administration

***Ernest Espinoza***  
Acting Chief Executive Officer  
Long Beach Comprehensive Health Center

***Kim Hart***  
Information Systems Analyst  
Information Systems Administrative Services

***Maria Manquero***  
Information Systems Analyst  
Information Systems Administrative Services

***Sandy Mungovan***  
Dir. Information Systems Administrative  
Services and HIPAA Security Coordinator

***Reginald Roberts***  
HIPAA Security Support  
Information Systems Administrative Services

***Hung Tu***  
Director  
Information Systems Technology Services

***Benjamin Wade***  
HIPAA Security Support  
Information Systems Administrative Services

***Tom Aki***  
Project Manager  
Information Systems Administrative Services

***Diane Barnett***  
Information Systems Analyst  
Information Systems Services

***Kenneth Duong***  
Technical Security  
Information Technology Services

***Judy Hardy***  
Human Resources

***Tony Hayden***  
Sergeant  
County Police

***Jeanette Miura, R.N.***  
Director, Fiscal & Management Systems  
Department of Nursing

***Julie Rees***  
Assistant Administrator  
Hospital Administration

***Donna Samuels, ART***  
Assistant Director  
Health Information Management

***Susie Ukkestad***  
Supervisor  
Department of Pathology

**PUBLICATION SUPPORT**

Maria Puga  
Information Systems Administrative Services

## **PREFACE**

The format of the Health Insurance Portability and Accountability Act (HIPAA Security Standard) "Security Rule" Comprehensive Self-Study Guide has been organized to reflect Harbor-UCLA Medical Center's (Harbor) and Coastal Cluster Health Centers' (CCHC) commitment to adult learning in educational programs. Each workforce member is required to read the study guide and successfully complete the assessment. Additional specialized training will be required of the Chief Information Officer (CIO), System Manager/Owner, System Administrators and Information Technology (IT) staff.

### **Objectives:**

Upon completion of this section, the participant will be able to:

1. Identify how the security standards safeguard individual Protected Health Information (PHI) from misuse and/or unauthorized disclosure.
2. Recognize and become familiar with Harbor-UCLA Medical Center and DHS HIPAA security related policies.
3. Determine specific responsibilities for ensuring confidentiality of PHI.

### **Instructions for Completing:**

1. Review the content in each section.
2. Complete the HIPAA Security Comprehensive Assessment Questions provided separately. Record your responses on the HIPAA Security Comprehensive Assessment Answer Sheet.
3. Check your responses against the answer key provided for each question. For those questions missed, review the Self-Study Guide for the correct answers.
4. Return the answer sheet to your the supervisor/training coordinator.
5. Supervisors/training coordinators are to forward the completed answer sheets to:  
Information Systems  
Building 3.5, Box 503  
Attention: Maria Puga  
As training is mandatory, it is recommended that copies of the completed answer sheet be kept in your departmental employee training files.
6. Information Systems will track completion of training and submit report to Health Services Administration for Board of Supervisor Reporting.

## Definitions:

Workforce Member	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.
System Managers/Owners	The person who is responsible for the operation and use of a system.
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.
Hybrid Covered Entity	A single legal entity that acts as provider and health care plan.

## I. INTRODUCTION

In 1996, the Health Insurance Portability and Accountability Act (HIPAA) became law.

In 2003, DHS began conducting HIPAA privacy and confidentiality training to implement the first phase of the HIPAA regulations. HIPAA includes several implementation phases, one of which is the HIPAA security rule. The purpose of this self-study guide is to provide Instruction on the “security rule” as it pertains to Harbor-UCLA Medical Center / Coastal Cluster Health Centers’. HIPAA Privacy and Security Training Program.

Everyone who works in the health care industry needs to be familiar with these rules. The question we all must ask ourselves is, “In what ways am I responsible for securing Protected Health Information?” Securing protected health information sounds like it should be simple, but meeting the legal requirements is not always easy.

The law contains numerous regulations covering the treatment of health information and affects how health care workers do their jobs. The requirements of HIPAA are detailed and the penalties for violating the rules are severe. There are three components under the HIPAA that contain requirements specific to health care organizations:

1. Standards for the Privacy of Individually Identifiable Health Information
2. Standards for Electronic Security
3. Standards for Electronic Transactions and Code Sets

This self-study guide focuses on the HIPAA Standards for Electronic Security Rules (“Security Rules”) and how the Los Angeles County Department of Health Services

(DHS), Harbor and CCHC policies comply with the rules. All workforce members must complete HIPAA Security training, which is covered by the material in this self-study guide. Security awareness materials such as newsletters and pamphlets are used to supplement the comprehensive training.

The CIO, System Manager/Owner, System Administrators and IT staff must complete additional specialized training to ensure systems meet minimum DHS security measures. The specialized procedural training will pertain to routine system maintenance and downtime procedures, risk assessment, system management and access control, data security and Business Continuity & Disaster Recovery Plans as they relate to each specific system.

The basic purpose of the HIPAA Security Rule is to protect the confidentiality, integrity and availability of electronic Protected Health Information (PHI) when it is collected, maintained, used or transmitted. This includes putting security measures in place to control access to electronic PHI and to protect such information from alteration, destruction, loss, and accidental or intentional disclosure to unauthorized persons.

The Security Rule applies to Covered Entities who collect, maintain, use or transmit protected health information in electronic form. Covered Entities include:

- Health Plans
- Health Care Clearinghouses
- Health Care Providers

The Los Angeles County is considered a Hybrid Covered Entity (see glossary) that includes:

- Department of Health Services
- Department of Mental Health
- Sheriffs' Department (Medical Facilities)
- Probation Department (Kirby Center)

## **II. HIPAA Security Rule**

The HIPAA Security Rule covers electronic PHI at rest (which means in storage), as well as during transmission (which means sending electronically). Any electronic PHI that is received, created, transmitted or maintained by Harbor and/or CCHC is included under the Rule.

Harbor and CCHC must provide safeguards for the following:

- Computer hardware and software
- Locations that house computer hardware and software
- Storage and disposal of data
- Back-up of data
- Access to data

- Maintenance of facilities
- Visitor access to facilities

Patients do not have to ensure that information they send to us electronically is secure; for example, in an e-mailed message. However, once a patient's email containing PHI is received by Harbor or the CCHC, it must be protected in accordance with the Security Rule and policy. PHI must not be communicated through e-mail outside of the DHS Network (e.g., across the Internet). PHI can be transmitted within DHS using the secured DHS Network and GroupWise if necessary for treatment, operations or payment.

The Security Rule covers all electronic media. Electronic media includes:

- Computer networks, desktop computers, laptop computers, personal digital assistants, handheld computers,
- Computer software applications,
- Magnetic tapes, disks, compact disks, USB storage devices and other means of storing electronic data, and
- Telephone voice response, "fax back" and other systems that are used as input and output devices for computers.

Paper-to-paper, person-to-person telephone calls, video teleconferencing or messages left on voice mail are not covered by the Security Rule; however, these and other methods of transmission of PHI not listed as electronic media are covered under HIPAA Privacy. Questions regarding HIPAA privacy should be referred to our HIPAA Privacy Coordinator or HIPAA Compliance Officer.

A HIPAA Security Officer is required to oversee security implementation and enforcement of the Security Rule. The Security Officer guides the organization in determining the best ways to implement the Security Rule. (See Appendix A for a list of the HIPAA Security Officers and Coordinators).

The Centers for Medicare and Medicaid Services (CMS) is responsible for ensuring compliance with the Security Rule. Suspected violations are reported to the Office of Inspector General. The Office of Inspector General will investigate and may recommend penalties up to \$250,000 and/or 10 years in jail.

The Security Rule is comprised of the following three categories of standards:

- Administrative Safeguards
- Physical Safeguards, and
- Technical Safeguards

Each Standard has implementation specifications. There are two (2) types of implementation specifications:

- Required (R) Must be followed as they are written in the Security Rule and cannot be determined to be unreasonable or inappropriate for the organization.

- Addressable (A) Must be implemented if reasonable and appropriate for the organization. If not implemented, an explanation for why it was not reasonable or appropriate must be provided. An alternative mechanism may be used to meet the standard. *(Note: “Addressable” does NOT mean optional. These must be addressed either through implementation or explanation.)*

Appendix B provides a summary for each of the three safeguards and related Harbor and DHS Security policies/procedures, standards and guidelines.

## A. Administrative Safeguards

Administrative Safeguards require written documentation of the security measures. Policies and procedures must ensure prevention, detection, containment and correction of security violations. Policies and procedures must also ensure that all workforce members have appropriate access to electronic PHI in order to perform their job.

These documented measures, policies and procedures must be kept on file for at least six years and updated through periodic review. A review might be triggered by an established review cycle, a change in technology, or a new security threat or incident.

The Security Rule requires that each organization implement Administrative Safeguard policies and procedures regarding:

- **Risk Analysis** - an accurate review of the risks involved in meeting the confidentiality, integrity and availability of PHI requirements;
- **Risk Management** - implementation of security measures that will reduce the risks of attacks or losses that were identified in the risk analysis;
- **Sanction/Disciplinary actions** - imposed on individuals for security violations;
- **Information Systems Activity Review procedures** - regular review of information system activity records, including audit logs and security incident tracking reports;
- **Security Incident Reporting and Response** addressing:
  - Actions that are considered security incidents;
  - The process to document such incidents;
  - The information that should be included in the documentation;
  - Appropriate responses for different types of incidents;
- **Contingency Plan** - response to computer system emergencies:
  - Data back-up - create and maintain retrievable exact copies of electronic PHI;
  - Disaster recovery plan - procedures to restore any loss of data;
  - Emergency mode operations plan - procedures that make it possible to continue critical business activities that protect the security of electronic PHI during an emergency; and

- **Business Associate Contracts and other Arrangements (i.e., MOU, Purchase Orders)** - Contracts and other arrangements between DHS and outside entity that create, receive, maintain or transmit electronic PHI on behalf of DHS.

## B. Physical Safeguards

Physical safeguards protect Harbor's and Coastal Cluster Health Centers' electronic information system hardware and related buildings and equipment. Security measures include protections from natural or environmental hazards and unauthorized access.

An organization must implement policies and procedures to:

- Limit physical access to electronic information systems and the building(s) in which they are kept.
- Restrict access to computers or computer systems containing electronic PHI to authorized users, e.g., passwords.
- Assign security responsibilities to individuals who will supervise the use of approved security measures.
- Limit access to data viewed on workstations, e.g., logging off the computer before leaving a workstation and automatic time-outs.
- Dispose of or re-use of electronic media containing electronic PHI.

## C. Technical Safeguards

Technical safeguards include the use of computer technology solutions to protect the integrity, confidentiality and availability of electronic PHI.

The Technical Safeguard standards require written documentation of security measures, policies and procedures implemented with respect to:

- **Access Control** - ensures appropriate technical solutions are in place to protect the integrity, confidentiality and availability of electronic PHI.
- **Audit Control** - requires implementation of hardware, software, and/or procedures that record and examine activity in information systems containing or using electronic PHI.
- **Integrity** – prevents electronic PHI from being improperly altered or destroyed.
- **Person or Entity Authentication** - procedures to verify that a person or entity seeking access to electronic PHI is the one he, she or it is claiming to be.
- **Transmission Security** - protects against unauthorized access to electronic PHI while it is being transmitted.

### **III. HIPAA vs. State Law**

HIPAA and State law overlap in many areas. Always follow the more stringent rule.

### **IV. Conclusion**

The basic purpose of the HIPAA Security Rule is to protect the confidentiality, integrity and availability of electronic PHI. Therefore, each workforce member must be aware of the appropriate security measures to reduce the risk of improper access, uses, and disclosures of electronic PHI. Measures such as virus protection, monitoring login success/failure, reporting of discrepancies, and password management are covered under DHS and Facility policies and procedures.

Be familiar with and follow all applicable policies and procedures. If you have any questions regarding the protection of electronic PHI, contact Harbor's HIPAA Security coordinator. Or Health Center Administration.

**Los Angeles County – Department of Health Services  
HIPAA Security Officers  
HIPAA Security and Training Coordinators**

Los Angeles County	Al Brusewitz Chief Information Security Officer County of Los Angeles, Chief Information Office 9150 East Imperial Highway Downey, CA 90063
Department of Health Services	Paul Fu, Jr., M.D. DHS HIPAA Security Officer 313 N. Figueroa Street Los Angeles, CA 90012
Harbor-UCLA Medical Center and Coastal Cluster Health Centers	Miguel Ortiz-Marroquin HIPAA Compliance Officer 1000 W. Carson Street, Box 1 Torrance, CA 90509 310-222-2104
Harbor-UCLA Medical Center and Coastal Cluster Health Centers	Sandy Mungovan HIPAA Security Coordinator Co-Chair, HIPAA Security Team 1000 W. Carson Street, Box 41 Torrance, CA 90509 310-222-5448
Harbor-UCLA Medical Center and Coastal Cluster Health Centers	Julie Rees Co-Chair, HIPAA Security Team 1000 W. Carson Street, Box 1 Torrance, CA 90509 310-222-2104
Harbor-UCLA Medical Center and Coastal Cluster Health Centers	Alma Smith HIPAA Privacy Coordinator 1000 W. Carson Street, Box 503 Torrance, CA 90509 310-222-2045

**HARBOR-UCLA MEDICAL CENTER / COASTAL CLUSTER HEALTH CENTERS  
HIPAA SECURITY  
POLICY AND PROCEDURES SUMMARY**

**NOTE:** Harbor-UCLA Medical Center and DHS policy and procedures are referenced below. The Harbor policy & procedures are effective April 21, 2005. Complete copies of Harbor policy and procedures can be found on the Harbor Intranet or in your department’s copy of the Harbor Policy and Procedure Manual. Contact your CCHC Administrator for CCHC specific policies. DHS Policy and Procedures can be found on the DHS Intranet Website ([www.ladhs.org](http://www.ladhs.org)).

<b>IMPORTANT DHS INFORMATION SECURITY POLICIES FOR WORKFORCE MEMBERS</b>				
<b>Standards</b>	<b>Implementation Specifications &amp; Type</b>	<b>Harbor &amp; DHS Policy Numbers &amp; Title</b>	<b>DHS Policy Purpose</b>	<b>Accountability</b>
		<p>731: Information Technology and Security Policy</p> <p>DHS Cross Reference: 935.00: DHS Information Technology and Security Policy</p>	<p>To provide direction for the development and implementation of data security policies and procedures and to identify the data security officials and their responsibilities.</p> <p>DHS and each facility are responsible for securing all electronic data including PHI and must also comply with all regulatory, compliance and accreditation sources such as HIPAA and JCAHO.</p> <p>Harbor and CCHC workforce members must comply with the provisions of DHS, local facility data security policies</p>	<p>DHS Information Security Officer</p> <p>Chief Information Officer</p> <p>Information Security Coordinators</p> <p>System Managers / Owners</p> <p>DHS Human Resources</p> <p>Workforce Members</p>

HARBOR-UCLA MEDICAL CENTER / COASTAL CLUSTER HEALTH CENTERS

HIPAA SECURITY  
POLICY AND PROCEDURES SUMMARY

**IMPORTANT DHS INFORMATION SECURITY POLICIES FOR WORKFORCE MEMBERS**

<b>Standards</b>	<b>Implementation Specifications &amp; Type</b>	<b>Harbor &amp; DHS Policy Numbers &amp; Title</b>	<b>DHS Policy Purpose</b>	<b>Accountability</b>
Workforce Security	Authorization and/or Supervision  Workforce Clearance Procedure  Termination Procedures	734: Workforce Security  DHS Cross Reference: 935.03: Workforce Security	To ensure 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).  Ensures access to information systems that contain PHI or other confidential information is given to workforce members based on their job responsibilities and “need to know”.	Chief Information Officer  System Managers/ Owners  Workforce Members

HARBOR-UCLA MEDICAL CENTER / COASTAL CLUSTER HEALTH CENTERS

HIPAA SECURITY  
POLICY AND PROCEDURES SUMMARY

**IMPORTANT DHS INFORMATION SECURITY POLICIES FOR WORKFORCE MEMBERS**

Standards	Implementation Specifications & Type	Harbor & DHS Policy Numbers & Title	DHS Policy Purpose	Accountability
Security Incident Procedures	Response and Reporting	<p>737: Security Incident Report and Response</p> <p>DHS Cross Reference: 935.06: Security Incident Report and Response</p>	<p>To develop, implement and maintain appropriate security incident identification, response, mitigation, and related documentation processes.</p> <p>Requires each workforce member to immediately report any and all suspected and actual breaches of information security to the Information Security Coordinator (310-222-5448) and Information Technology Services Director (310-222-5059). Security incidents include, but are not limited to virus attacks, unauthorized access to electronic system containing PHI, or theft of electronic equipment storing PHI.</p> <p>Information Security Coordinator and Information Technology Services Director to follow appropriate escalation and reporting procedures to DHS Information Security Officer and Department Cyber-terrorism Emergency Response Team.</p>	<p>Workforce Members</p> <p>Information Security Coordinator</p> <p>Information Technology Services Director</p>

HARBOR-UCLA MEDICAL CENTER / COASTAL CLUSTER HEALTH CENTERS

HIPAA SECURITY  
POLICY AND PROCEDURES SUMMARY

**IMPORTANT DHS INFORMATION SECURITY POLICIES FOR WORKFORCE MEMBERS**

Standards	Implementation Specifications & Type	Harbor & DHS Policy Numbers & Title	DHS Policy Purpose	Accountability
Workstation Use/Workstation Security	Workstation Use Workstation Security	742: Workstation Use and Security  DHS Cross Reference: 935.11:Workstation Use and Security	<p>To restrict workstation use and access to Protected Health Information (PHI) and other confidential information by using physical, administrative, and technical controls.</p> <p>Requires all users to take reasonable security precautions to prevent unauthorized physical access to sensitive information from workstations (e.g., concealing video displays, securing Unattended workstations by using password protected screensavers, etc.).</p> <p>Requires workstations to be password protected.</p> <p>Workstation must be positioned away from common areas or have privacy screen installed.</p> <p>Mobile devices must be pre-approved by the CIO; require encryption for sensitive information; must not be left unattended in a non-secure area; if left in car, must be locked in the car and stored out-of-sight.</p>	<p>Chief Information Officer</p> <p>System Managers/ Owners</p> <p>Workforce Members</p>

HARBOR-UCLA MEDICAL CENTER / COASTAL CLUSTER HEALTH CENTERS

HIPAA SECURITY  
POLICY AND PROCEDURES SUMMARY

**IMPORTANT DHS INFORMATION SECURITY POLICIES FOR WORKFORCE MEMBERS**

Standards	Implementation Specifications & Type	Harbor & DHS Policy Numbers & Title	DHS Policy Purpose	Accountability
Workstation Use/Workstation Security (Cont.)			<p>Confidential Information is not to be stored or saved on removable media (floppy disks, USB drives, etc.) without proper safeguards and authorization; removable media must be maintained or stored in a secure area. Printers for confidential information must not be left unattended or in a non-secure area.</p> <p>Media and information must be disposed of properly.</p> <p>Workstations located in a public or open area must be physically secured in a locked room, locked cabinet or strongly anchored.</p> <p>Security cameras may be used in high-risk locations.</p> <p>Workforce members must not install/uninstall software (County installed, Internet software, games, screensavers, patches, plug-ins) or repair servers or workstations without authorization.</p>	

HARBOR-UCLA MEDICAL CENTER / COASTAL CLUSTER HEALTH CENTERS

HIPAA SECURITY  
POLICY AND PROCEDURES SUMMARY

**IMPORTANT DHS INFORMATION SECURITY POLICIES FOR WORKFORCE MEMBERS**

Standards	Implementation Specifications & Type	Harbor & DHS Policy Numbers & Title	DHS Policy Purpose	Accountability
Person or Entity Authentication	Person or Entity Authentication	748: System, Person or Entity Authentication  DHS Cross Reference: 935.17: System, Person or Entity Authentication	To verify that a person or entity seeking access to Protected Health Information (PHI) and other confidential information is the one claimed.  Directs workforce members not to use another person's user ID/code, password, or other security device to gain access to an information system. Requires workforce members to verify the identity of any person or entity receiving PHI or other confidential information.  Requires the CIO to ensure that a workforce member is the actual person he/she claims to be.	Workforce Members  Chief Information Officer  DHS Information Security Officer

HARBOR-UCLA MEDICAL CENTER / COASTAL CLUSTER HEALTH CENTERS

HIPAA SECURITY  
POLICY AND PROCEDURES SUMMARY

**IMPORTANT DHS INFORMATION SECURITY POLICIES FOR WORKFORCE MEMBERS**

Standards	Implementation Specifications & Type	Harbor & DHS Policy Numbers & Title	DHS Policy Purpose	Accountability
		<p>627: Data Security Responsibility</p> <p>DHS Cross Reference: 935.20: Acceptable Use Policy for County Information Technology Resources</p>	<p>To ensure the proper use of County information technology resources within Harbor-UCLA Medical Center.</p> <p>This policy advises workforce members on the proper use of DHS' and the County's information technology resources. Workforce members are required to sign the County agreement containing information on the County's expectations on the use of information technology resources. Workforce members are also required to sign an acknowledgment that they have received the policy and the agreement. Both signed documents will be filed in the employee's official personnel file. Newly hired workforce members will be required to sign the agreement and acknowledgment at their new hire orientation.</p>	<p>Workforce Members</p>

HARBOR-UCLA MEDICAL CENTER / COASTAL CLUSTER HEALTH CENTERS

HIPAA SECURITY  
POLICY AND PROCEDURES SUMMARY

<b>ADDITIONAL ADMINISTRATIVE SAFEGUARDS POLICIES</b>				
<b>Standards</b>	<b>Implementation Specifications &amp; Type</b>	<b>Harbor &amp; DHS Policy Numbers &amp; Title</b>	<b>DHS Policy Purpose</b>	<b>Accountability</b>
Security Management Process	Risk Analysis	732: Security Management Process: Risk Management	To create and implement security management processes that ensure the security (confidentiality, integrity and availability) of Protected Health Information (PHI) and other confidential information.	Information Security Officer
	Risk Management			
	Sanction Policy	DHS Cross Reference: 935.01: Security Management Process: Risk Management	Requires System Managers/Owners to analyze the security risk levels for each of their information systems and develop procedures to decrease the chance that the systems will be attacked by a virus or accessed by unauthorized users. They are also required to identify steps to minimize any damage to systems and contents in the event of such occurrence.	Chief Information Officer
	Information System Activity Review			
	Workforce Clearance Procedure			
Termination Procedures			System Managers / Owners	

HARBOR-UCLA MEDICAL CENTER / COASTAL CLUSTER HEALTH CENTERS

HIPAA SECURITY  
POLICY AND PROCEDURES SUMMARY

<b>ADDITIONAL ADMINISTRATIVE SAFEGUARDS POLICIES</b>				
<b>Standards</b>	<b>Implementation Specifications &amp; Type</b>	<b>Harbor &amp; DHS Policy Numbers &amp; Title</b>	<b>DHS Policy Purpose</b>	<b>Accountability</b>
Information Access Management	Isolating Health care Clearinghouse Function  Access Authorization  Access Establishment and Modification	735: Information Access Management  DHS Cross Reference: 935.04:Information Access Management	To create administrative controls for access to Protected Health Information (PHI) and other confidential and/or sensitive information. To restrict access to those persons and external entities with a need for access is a basic tenet of security.  Establish mechanisms and procedures requiring System Managers/Owners to develop and implement policies and procedures to grant/restrict access to systems based on “need-to-know” basis, and job responsibilities. The policy also addresses the manner by which information may be accessed (workstation, transaction, program, process), who can grant access to systems, and the monitoring of authorized persons who need to work in areas containing PHI.	Chief Information Officer  System Managers / Owners

HARBOR-UCLA MEDICAL CENTER / COASTAL CLUSTER HEALTH CENTERS

HIPAA SECURITY  
POLICY AND PROCEDURES SUMMARY

**ADDITIONAL ADMINISTRATIVE SAFEGUARDS POLICIES**

Standards	Implementation Specifications & Type	Harbor & DHS Policy Numbers & Title	DHS Policy Purpose	Accountability
Security Awareness and Training	Security Reminders  Protection from Malicious Software  Log-in Monitoring  Password Management	701: Privacy and Security Awareness Training  DHS Cross Reference: 361.24: Privacy and Security Awareness Training	To outline the Privacy and Security training for the Harbor-UCLA Medical Center.  Requires all workforce members to be trained on their responsibilities related to protecting the confidentiality, integrity and availability of PHI and other confidential information  The types of training are as follows: <ul style="list-style-type: none"> <li>• Awareness - distributing information related to privacy and security issues;</li> <li>• Comprehensive training - role-based for privacy; all staff for security issues;</li> <li>• Specialized training - for specific workforce members who handle and maintain information systems; and</li> <li>• Business Associates for those who provide contract and purchase order services.</li> </ul>	Chief Information Officer

HARBOR-UCLA MEDICAL CENTER / COASTAL CLUSTER HEALTH CENTERS

HIPAA SECURITY  
POLICY AND PROCEDURES SUMMARY

<b>ADDITIONAL ADMINISTRATIVE SAFEGUARDS POLICIES</b>				
<b>Standards</b>	<b>Implementation Specifications &amp; Type</b>	<b>Harbor &amp; DHS Policy Numbers &amp; Title</b>	<b>DHS Policy Purpose</b>	<b>Accountability</b>
Security Awareness and Training (Cont.)			<p>Training includes providing workforce members with periodic security updates; procedures for protecting information systems from malicious software such as viruses and worms; procedures for monitoring computer or network log-in attempts and reporting discrepancies; and procedures for creating, changing and safeguarding passwords</p> <p>The policy also addresses safeguarding passwords, user id's and other security identification devices; workstation usage; new hire orientation; facility orientation; job specific training each time workforce member changes job responsibilities and any time HIPAA privacy or data security rules are revised, and whenever general data security policies or procedures need to be revised.</p>	

HARBOR-UCLA MEDICAL CENTER / COASTAL CLUSTER HEALTH CENTERS

HIPAA SECURITY  
POLICY AND PROCEDURES SUMMARY

<b>ADDITIONAL ADMINISTRATIVE SAFEGUARDS POLICIES</b>				
<b>Standards</b>	<b>Implementation Specifications &amp; Type</b>	<b>Harbor &amp; DHS Policy Numbers &amp; Title</b>	<b>DHS Policy Purpose</b>	<b>Accountability</b>
Contingency Plan	Data Backup Plan Disaster Recovery Plan  Emergency Mode Operation Plan  Testing and Revision Procedure  Applications and Data Criticality Analysis	738: Facility Information Technology (IT) Contingency Plan  DHS Cross Reference: 935.07: Facility Information Technology (IT) Contingency Plan	To define the Facility Information Technology (IT) Contingency plan.  Requires each DHS facility to develop and implement an IT Contingency Plan (a master plan for responding to IT system emergencies (e.g., fire, vandalism, system failure, and natural disaster)) to ensure that facility/departmental operations can continue with minimal interruption and data recovery. The elements contained in the plan must be based on how important the system is to the facility/department and must address issues such as data backup and recovery, and identification of emergency response personnel and responsibilities.	Chief Information Officer  System Managers / Owners

HARBOR-UCLA MEDICAL CENTER / COASTAL CLUSTER HEALTH CENTERS

HIPAA SECURITY  
POLICY AND PROCEDURES SUMMARY

ADDITIONAL ADMINISTRATIVE SAFEGUARDS POLICIES				
Standards	Implementation Specifications & Type	Harbor & DHS Policy Numbers & Title	DHS Policy Purpose	Accountability
Evaluation	Evaluation	739: Security Compliance Evaluation  DHS Cross Reference: 935.08: Security Compliance Evaluation	To establish a process for monitoring Harbor's compliance with the security aspects of the <u>Harbor Policy No. 700: Harbor-UCLA Medical Center Privacy and Security Compliance Program</u> .  Requires each Harbor to annually evaluate IT security safeguards to ensure they are in compliance with the data security and risk management requirements. One of the safeguards (administrative, technical, physical) must be reviewed each year for each system.	Chief Information Officer  Information Security Coordinator  Privacy Coordinator

HARBOR-UCLA MEDICAL CENTER / COASTAL CLUSTER HEALTH CENTERS

HIPAA SECURITY  
POLICY AND PROCEDURES SUMMARY

ADDITIONAL ADMINISTRATIVE SAFEGUARDS POLICIES				
Standards	Implementation Specifications & Type	Harbor & DHS Policy Numbers & Title	DHS Policy Purpose	Accountability
Business Associate Contracts and Other Arrangements	Written Contract or Other Arrangement	725 Business Associate Agreement  DHS Cross Reference: 361.20: Business Associate Agreement	<p>To protect individuals' Protected Health Information (PHI) transferred to, created or received by the Harbor-UCLA Medical Center's Business Associates by requiring contractual assurances that the Business Associate will safeguard the Protected Health Information and use the Protected Health Information only as permitted by the Business Associate agreement.</p> <p><u>Applicability:</u> This policy relates to relevant Board of Supervisor's Agreements and Purchase Orders executed by DHS for services by vendors (i.e., persons or entities) that perform functions, activities or services, other than treatment, on behalf of DHS that involve the use and/or disclosure of protected health information.</p> <p>DHS policy prohibits its officers and agents from disclosing PHI to any Business Associate without a written agreement. The written agreement directs the Business Associate on how it may use or disclose the PHI and its responsibilities to safeguard the information. The policy contains actual contract language for Business Associates that covers use and disclosure of PHI.</p>	Contract Management Director

HARBOR-UCLA MEDICAL CENTER / COASTAL CLUSTER HEALTH CENTERS

HIPAA SECURITY  
POLICY AND PROCEDURES SUMMARY

<b>ADDITIONAL PHYSICAL SAFEGUARDS POLICIES</b>				
<b>Standards</b>	<b>Implementation Specifications</b>	<b>DHS Policy No, &amp; Title</b>	<b>DHS Policy Purpose</b>	<b>Accountability</b>
Facility Access Controls	Contingency Operations  Facility Security Plan  Access Control Plan and Validation Procedures  Maintain Records  Workstation Security	741: Facility Access Control  DHS Cross Reference: 935.10: Facility Access Control	To define the process for ensuring the physical protection of Harbor's information systems and infrastructure.  Requires Harbor to implement policies that limit physical access to electronic information systems and the facilities in which they are housed. System access must be validated based on the workforce members' functions. The validation also applies to visitors. The policy also addresses security of software programs, the interior and exterior of premises, and equipment.	Chief Information Officer  System Managers / Owners

HARBOR-UCLA MEDICAL CENTER / COASTAL CLUSTER HEALTH CENTERS

HIPAA SECURITY  
POLICY AND PROCEDURES SUMMARY

<b>ADDITIONAL PHYSICAL SAFEGUARDS POLICIES</b>				
<b>Standards</b>	<b>Implementation Specifications</b>	<b>DHS Policy No, &amp; Title</b>	<b>DHS Policy Purpose</b>	<b>Accountability</b>
Device and Media Control	Disposal & Media Re-Use  Accountability  Data Backup and Storage	744: Device and Media Controls  DHS Cross Reference: 935.13:Device and Media Controls	The purpose of this policy is to state the requirement for controls that govern the receipt and removal of hardware and/or software (for example, diskettes and tapes) into and out of Harbor.  Requires System Managers/Owners to document the receipt, removal, reuse, and disposal of system hardware and software and to take certain precautions to make sure PHI or other confidential information are removed as necessary.	System Manager / Owners

HARBOR-UCLA MEDICAL CENTER / COASTAL CLUSTER HEALTH CENTERS

HIPAA SECURITY  
POLICY AND PROCEDURES SUMMARY

<b>ADDITIONAL PHYSICAL SAFEGUARDS POLICIES</b>				
<b>Standards</b>	<b>Implementation Specifications</b>	<b>DHS Policy No, &amp; Title</b>	<b>DHS Policy Purpose</b>	<b>Accountability</b>
Access Control	Unique User Identification  Emergency Access Procedure  Automatic Logoff  Encryption and Decryption	745: System Access Control  DHS Cross Reference: 935.14: System Access Control	This policy states the technical security requirements for electronic information systems to only allow access to persons or software programs that have appropriate access rights.  Describes security measures the System Manager/Owners must use to ensure the security of information systems (e.g., assigning unique user names, monitoring system log-in, automatic log-off, encryption/decryption, and maintaining system security documentation).	Chief Information Officer  System Manager/Owners

HARBOR-UCLA MEDICAL CENTER / COASTAL CLUSTER HEALTH CENTERS

HIPAA SECURITY  
POLICY AND PROCEDURES SUMMARY

<b>ADDITIONAL PHYSICAL SAFEGUARDS POLICIES</b>				
<b>Standards</b>	<b>Implementation Specifications</b>	<b>DHS Policy No, &amp; Title</b>	<b>DHS Policy Purpose</b>	<b>Accountability</b>
Audit Controls	Audit Controls	746: System Audit Control  DHS Cross Reference: 935.15: System Audit Control	To ensure audit control mechanisms that record and examine system activity are in place for all departmental electronic information systems.  Requires Harbor to log and store system activity and develop an “audit control and review plan” to determine which activities need to be monitored, the responsibilities of applicable workforce members, and the frequency of audits.	Chief Information Officer  System Managers / Owners

HARBOR-UCLA MEDICAL CENTER / COASTAL CLUSTER HEALTH CENTERS

HIPAA SECURITY  
POLICY AND PROCEDURES SUMMARY

ADDITIONAL PHYSICAL SAFEGUARDS POLICIES				
Standards	Implementation Specifications	DHS Policy No, & Title	DHS Policy Purpose	Accountability
Integrity	Mechanism to Authenticate Electronic Protected Health Information	747: Information Integrity  DHS Cross Reference: 935.16: Information Integrity	To protect Protected Health Information (PHI) and other confidential information from improper alteration and/or destruction.  Requires the CIO, and System Manager/Owners to take appropriate authentication measures based on the systems' risk level to ensure data and information contained in systems is not intentionally altered or destroyed. Requires workforce members to report any unauthorized destruction or alteration of data to the system manager/owner.	DHS Information Security Officer  Chief Information Officers  System Managers/Owners  Workforce Members

HARBOR-UCLA MEDICAL CENTER / COASTAL CLUSTER HEALTH CENTERS

HIPAA SECURITY  
POLICY AND PROCEDURES SUMMARY

<b>ADDITIONAL PHYSICAL SAFEGUARDS POLICIES</b>				
<b>Standards</b>	<b>Implementation Specifications</b>	<b>DHS Policy No, &amp; Title</b>	<b>DHS Policy Purpose</b>	<b>Accountability</b>
Transmission Security	Integrity Controls  Encryption	749: Transmission Security Policy  DHS Cross Reference: 935.18 Transmission Security Policy	To state the technical requirement that electronic information transmitted over a communications network must be protected in a manner commensurate with the associated risk.  Requires Harbor to take appropriate measures such as encryption to ensure the security of information transmitted electronically over the Internet, external communications and all parts of a communications network.	DHS Information Security Officer  Chief Information Officer  System Managers/Owners

HARBOR-UCLA MEDICAL CENTER / COASTAL CLUSTER HEALTH CENTERS

HIPAA SECURITY  
POLICY AND PROCEDURES SUMMARY

OTHER RELATED DHS SECURITY POLICIES AND PROCEDURES

Harbor Policy No.	Policy Title	Policy Purpose	Accountability
	<p>700: Harbor-UCLA Medical Center Privacy and Security Compliance Program</p> <p>DHS Cross Reference: 361.1: Department of Health Services Privacy and Security Compliance Program</p>	<p>To define the Privacy and Security Program for Harbor-UCLA Medical Center</p> <p>Summarizes the elements of the DHS Privacy and Security Program which includes:</p> <ul style="list-style-type: none"> <li>• Training of workforce members</li> <li>• Disciplinary action for failure to follow privacy and security policies</li> <li>• Development of policies and procedures to safeguard all aspects of PHI and other confidential information</li> <li>• Whistleblower and workforce crime victims protections</li> <li>• Mitigation, non-retaliation, the complaint process, implementation, and documentation</li> <li>• Assignment of responsibility to implement and enforce policies and procedures protecting PHI and other confidential information.</li> </ul>	<p>Workforce Members</p>
	<p>706: Safeguards for Protected Health Information</p>	<p>To establish safeguards that must be implemented by Harbor-UCLA Medical Center to protect the confidentiality of protected health information.</p> <p>Describes the minimum standards for ensuring the</p>	<p>Workforce Members</p>

HARBOR-UCLA MEDICAL CENTER / COASTAL CLUSTER HEALTH CENTERS

HIPAA SECURITY  
POLICY AND PROCEDURES SUMMARY

Harbor Policy No.	Policy Title	Policy Purpose	Accountability
	<p>DHS Cross Reference: 361.23: Safeguards for Protected Health Information</p>	<p>confidentiality of Protected Health Information (PHI). The policy addresses: oral communications, cellular telephones, telephone messages, faxes, U.S. Mail, destruction standards, physical access to PHI, technical safeguards, use of electronic systems (i.e., PDAs, E-mail, WLANs, electronic transmission of clinical laboratory tests) and document retention.</p> <p>This policy requires each workforce member to sign acknowledgment of <u>DHS Guidelines Governing the Use of E-Mail Involving Protected Health Information (PHI)</u>.</p>	
	<p>750: Data Security Documentation Requirement</p> <p>DHS Cross Reference: 935.19: DHS Data Security Documentation Requirement</p>	<p>To establish documentation requirements for data security policies and procedures and for Health Insurance Portability and Accountability Act (HIPAA) Security Rule implementation decisions.</p> <p>Requires Harbor-UCLA Medical Center to maintain policies and procedures in paper or electronic form, and all other data security documentation, including security actions taken and assessments, for at least 6 years or as required by any regulatory, compliance and/or accreditation agency. Requires documents to be readily available to appropriate users and auditors.</p>	<p>Chief Information Officer</p>

HIPAA Security Comprehensive  
Frequently Asked Questions (FAQs)

***I have a poor memory and can't seem to remember passwords and user IDs, where is a safe place to keep them?***

A couple of things to remember when creating user IDs and passwords:

- Keep it simple enough for you to remember – relate it to a subject you enjoy or have an interest such as the title of a favorite book, song, food, old home address or any other topic that another individual would not associate with you. Do not use names of relatives, pets, sports teams, fictional characters, birthdates, employee number, or other easily guessed or looked up objects.
- Use a combination of letters and numbers and/or upper and lower case letters.

Passwords and user IDs may be written on paper and stored in a secure and/or locked location. Passwords and user IDs must not be stored in an unlocked desk, computer file or on the computer desktop, floppy disk stored on the desk, or posted inside the work area. Do not carry passwords in a purse or wallet.

***I received an e-mail with an attachment. The e-mail said my computer has been infected with a virus and instructed me to follow the directions and open the attachment to get rid of the virus. Should I follow the instructions?***

No. Never open unexpected attachments or follow instructions for handling a virus from anyone other than your Information Systems Unit. If you are unsure about whether you should open something, contact your Information Systems Unit.

***I am a new employee and have not been given a computer to work on yet. My supervisor gave me her user ID and password and instructed me to use this information to get on her computer to work with PHI. Should I use it?***

No. Your supervisor should not have given you his/her user ID and password to use. Instead, he/she should submit a request to your Information Systems Unit to get your own password and user ID. Furthermore, an employee should not log-in to a system to allow another employee access to the system. In both cases, the employee who is assigned the user ID and password would be liable for anything that happens to the system or information.

***My friend e-mailed a message to me containing a funny skit. Should I open it?***

No. Although your friend has good intentions, the e-mailed file may contain a virus or worm. County policy prohibits this type of use of the e-mail system and both employees may be subject to disciplinary action.

HIPAA Security Comprehensive  
Frequently Asked Questions (FAQs)

***Is it okay to store medical information on CD or floppy disk?***

If you're keeping PHI or any other confidential information on a CD or other storage media, it should be encrypted and kept in a secure location. Contact your Information Systems Unit to obtain advice and assistance on acquiring and using encryption software.

***I work in the business office of a health facility and a patient asks me to look up her recent test results. I do not have access to laboratory test results and the patient is demanding that she has rights to her medical information as stated in the Privacy Notice. Should I look in her paper chart or try to guess a co-worker's log-in information?***

Neither. Looking in the patient's medical chart or obtaining the information from guessing a co-worker's log-in information would be a security violation. Politely explain to the patient that protecting the privacy of her information is of utmost importance to the Department and that only the doctors and nurses have access to confidential information such as lab results. Inform her that you will take a message for her doctor or the nurse and have the doctor/nurse call her with the results. Provide the patient with the telephone number to contact and, if possible, the amount of time a doctor/nurse will need to respond.

***I work in an office that handles PHI on many different computer systems. Some systems automatically logoff after a few minutes of inactivity, others do not. We have been told to always logoff when we are away from our desk, but some employees fail to do so. Should I speak to anyone about this?***

Users must always logoff of systems containing PHI. You can talk to your Information Systems Unit or HIPAA Security Coordinator and let them know which systems do not have an automatic logoff feature.

***I have boxes of floppy disks and CDs that need to be discarded. How do I go about discarding them? Do I simply throw them in the trash? What do I do with the ones that contain PHI or other confidential information?***

All storage media must be irreversibly destroyed following the DHS Policy No. 935.13, Device and Media Control. Contact your Information Systems Unit or HIPAA Security Coordinator.

***I frequently use Instant Messenger to send user IDs and passwords to employees within my unit. Is this a safe and appropriate manner to communicate the information to employees?***

No, Instant Messenger is not appropriate for sending user IDs and passwords.