COUNTY OF LOS ANGELES

AGREEMENT FOR ACCEPTABLE USE AND CONFIDENTIALITY OF COUNTY'S INFORMATION TECHNOLOGY ASSETS, COMPUTERS, NETWORKS, SYSTEMS AND DATA

As a Los Angeles County, employee, contractor, vendor, or other authorized employee of County Information Technology (IT) assets including computers, networks, systems and data, I understand that I occupy a position of trust. I will use County IT assets for County management approved business purposes only and maintain the confidentiality of County's business and Citizen's private data. As an user of County's IT assets, I agree to the following:

1. Computer Crimes: I am aware of California Penal Code 502(c) – Comprehensive Computer Data Access and Fraud Act (attached). I will immediately report any suspected computer misuse or crimes to my Management.

2. Security Access Controls: I will not subvert or bypass any security measure or system which has been implemented to control or restrict access to computers, networks, systems or data. I will not share my computer identification codes (log-in ID, computer access codes, account codes, ID's, etc.) or passwords.

3. Approved Business Purposes: I will use the County's Information Technology (IT) assets including computers, networks, systems and data for County management approved business purposes only.

4. Online Web-based Document Sharing Services
   I will not use Online Web-based Document Sharing Services to collaborate with workforce members; to store and/or share DHS owned data.

5. UNAUTHORIZED APPLICATION OR SOFTWARE
   I will not download, install, or use any non-DHS approved application or software, such as Instant Messaging, Streaming Media, and Remote Access Services (e.g., LogMeIn, GoToMyPC).

6. Confidentiality: I will **not view, access, use or disclose** any County program code, data, information or documentation to any individual or organization unless specifically authorized to do so by the recognized information owner.

7. Computer virus and malicious code: I will not intentionally introduce any computer virus, worms or malicious code into any County computer, network, system or data. I will not disable or delete computer virus detection and eradication software on County computers, servers and other computing devices I am responsible for.

8. Offensive materials: I will not access or send any offensive materials, e.g., sexually explicit, racial, harmful or insensitive text or images, over County owned, leased or managed local or wide area networks, including the public Internet and other electronic mail systems, unless it is in the performance of my assigned job duties, e.g., law enforcement. I will report to my supervisor any offensive materials observed by me or sent to me on County systems.

9. Public Internet: I understand that the Public Internet is uncensored and contains many sites that may be considered offensive in both text and images. I will use County Internet services for approved County business purposes only, e.g., as a research tool or for electronic communication. I understand that the County's Internet services may be filtered but in my use of them I may be exposed to offensive materials. I agree to hold the County harmless should I be exposed to such offensive materials. I understand that my Internet activities may be logged, are a public record, and are subject to audit and review by authorized individuals.

10. Electronic mail and other electronic data: I understand that County electronic mail (e-mail), and data, in either electronic or other forms, are a public record and subject to audit and review by authorized individuals. I will comply with County and DHS e-mail use policy and use proper business etiquette when communicating over e-mail systems.

11. Copyrighted materials: I will not copy any licensed software or documentation except as permitted by the license agreement.

12. Passwords: **I understand that I am responsible for safeguarding my passwords for access to County information technology resources and am responsible for all transactions made using my password. I will not share my passwords or provide access to another individual using my password.**

13. Disciplinary action for non-compliance: I understand that my non-compliance with any portion of this Agreement may result in disciplinary action including my suspension, discharge, denial of service, and cancellation of contracts or both civil and criminal penalties.

CALIFORNIA PENAL CODE 502(c)
"COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT"

Below is a section of the "Comprehensive Computer Data Access and Fraud Act" as it pertains specifically to this Agreement. California Penal Code 502(c) is incorporated in its entirety into this Agreement by reference and all provisions of Penal Code 502(c) apply. For a complete copy, consult the Code directly at website www.leginfo.ca.gov/.

502. (c) Any person who commits any of the following acts is guilty of a public offense:

(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongly control or obtain money, property, or data.

(2) Knowingly accesses and without permission takes, copies or makes use of any data from a computer, computer system, or computer network, or takes or copies supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

(3) Knowingly and without permission uses or causes to be used computer services.

(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.

(5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network is in violation of this section.

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

(9) Knowingly and without permission uses the Internet domain name of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damages or causes damage to a computer, computer system or computer network.

LAC+USC HEALTHCARE NETWORK SUPPLEMENT TO

Recordable Mobile Devices and Removable Media: All recordable mobile and removable media that contain Protected Health Information or sensitive business information covered by HIPAA, Civil Code 1798.29 & 1798.82, must be managed and controlled. These devices include PDA's, USB flash drives, cellular phone, cameras and camera phones, removable hard disks, CD-R, CD-RW, DVD-R, DVD-RW and floppy disks.

Management and Control: I understand all information protected under HIPAA, California Civil Codes 1798.29 and 1798.82 and other non-public business information stored and accessible on recordable mobile devices and/or recordable storage must be managed and controlled. The use of recordable mobile devices must be recognized by the Department Head. Recordable storage media must be managed and controlled though the use of auditable inventory logs.

Please list all the electronic devices, i.e. CDROM, PDA, USB, etc, you expect to utilize when accessing, recording, capturing, storing or transmitting information protected under HIPAA, California Civil Codes 1798.29 and 1798.82 and other non-public business information.

1._____ 3._____
2._____ 4._____

ACKNOWLEDGMENT:

I acknowledge that I have received and read the Department of Health Services' Policy No. 935.20, DHS (LAC+USC Policy No. 457) Acceptable Use Policy for County Information Technology Resources and the County of Los Angeles Agreement of Acceptable Use and Confidentiality of County's Information Technology Assets, Computers, Networks, Systems and Data. I agree to abide by the provisions of the policy and the agreement. If I fail to comply with the policy and agreement, I will be subject to disciplinary action, up to and including discharge. If I have any questions concerning the policy or agreement, I will discuss them with my supervisor.

I HAVE READ AND UNDERSTAND THE ABOVE AGREEMENT:

Employee's Name	Employee's Signature	Ext.	Date

Employee's Job Title	Employee Number	E-mail Address

Manager's Name	Manager's Signature	Ext.	Date
Justin Gillenwater		9-7750	

Location – Room Number	Department Name
Burn Unit 5D & 5M	Surgery

After completing the form, please, fax it to the Information System office at **Fax# 323-441-8056.**

Distribution:
Original – Employee Official Personnel Folder
Duplicate – Retain in Departmental Area File for Personnel: employees, contractors, students, volunteers and agency personnel.

ACKNOWLEDGEMENT OF CONDITIONS OF APPOINTMENT

I have read LAC+USC Healthcare Network Policy No. 113 and agree to the following conditions of appointment.

- My sole employer is _____ , upon which I rely exclusively for payment of salary and any and all other benefits payable to me or on my behalf during the period of this employment. I understand and agree that I am not an employee of Los Angeles County for any purposes and that I do not have and will not acquire any rights or benefits of any kind from the County during the period of my work in County facility(ies).

- Los Angeles County appointment can be terminated, changed, or altered by the County at any time, with or without cause or prior notice. This policy includes and applies to, without limitation, alternation of status, and cannot be changed in any way except by written agreement between an individual appointee, employing/sponsoring entity and an officer of LAC+USC Healthcare Network who is authorized to bind the Network.

- Scope of Assignment:

  ☐ The scope of my assignment involves patient care activities for which I will maintain current licensure and/or certification without restriction and provide evidence to the Network and Appointing Authority.

  ☐ The scope of my assignment does not involve patient care duties.

- Liability insurance and workers compensation are the responsibility of my employer, unless otherwise contractually provided, and the County of Los Angeles shall be held harmless and will not defend in any action taken against me as a result of activities within the LAC+USC Healthcare Network.

- I must be free of communicable disease, including tuberculosis, hepatitis B, and varicella, and provide verifying evidence to LAC+USC Healthcare Network Employee Health Services as a prior condition of my appointment.

- I must complete safety training, within six months of appointment, as required by the LAC+USC Healthcare Network.

- Photo-identification badges issued by the Network and employer must be worn at all times, as defined in LAC+USC Network policies and procedures, and displayed to patients, County employees, and the public upon request.

- Research activities are confined to the specific requirements of the IRB-approved project assigned.

- I may not enter into any patient care or work area except as defined in my job description and, as applicable, IRB-approved research protocol. Exceptions must be approved in writing by the Chief Medical Officer and/or Associate Dean, Graduate Medical Education.

- **Patient records are confidential documents that shall be kept confidential and never be removed from the Network facility providing the patient's care. Patient records will not be photocopied without consent of the patient and the Director of Health Information Management.** Access to patient records for research is limited to records required for the specific IRB-approved research project assigned and must be under the direction of supervisor.

- Use of County resources (telephones, facsimile machines, computers, electronic mail, copiers, etc.) is restricted to activities required in my job description.

_____	_____	_____
Name (printed) and Signature	Employee No.	Date

As supervisor of appointee, I have personally reviewed with him/her the conditions of appointment and take responsibility for ensuring compliance.

Justin Gillenwater	Burn Unit 5D&5M	_____
Name (printed) and Signature	Department	Date

DEPARTMENT OF HEALTH SERVICES
COMPLIANCE AWARENESS TRAINING

CODE OF CONDUCT ACKNOWLEDGEMENT

Instructions: After you have completed the Compliance Awareness Training, please complete this Code of Conduct Acknowledgement And submit it to your supervisor or trainer.

Date:	**Please PRINT Name (Last Name, First):**	**Employee No:**	**Department Name:** General Surgery	**Pay Location:** 70
		Dept No: 160	**Work Area:** Burn Unit 5D & 5M	**Phone No:** 409-7750

I acknowledge that I have received the Department of Health Services' Code of Conduct and completed the Compliance Awareness Training. I Agree to abide by the Code of Conduct as it relates to my job responsibilities. I understand that non-compliance with the Code of Conduct can subject me to disciplinary action up to and including discharge from service.

Employee's Signature:_____ Date:_____
Supervisor's Name (Print):___**Justin Gillenwater**_____
Supervisor's Signature:_____ Date:_____

C: Workforce Member
Unit File
Official Personnel/Contractor File

Health Services
LOS ANGELES COUNTY

PRIVACY & SECURITY SURVIVAL TRAINING: PROTECTING PATIENT INFORMATION

ANSWER SHEET AND PROOF OF COMPLETION

Instructions: Please circle the correct letter corresponding with the questions in the study guide. You must score 20 correct to receive credit for Mandatory Training.

1.	A	B	C	D	E	11.	A	B	C	D	E
2.	A	B	C	D	E	12.	A	B	C	D	E
3.	A	B	C	D	E	13.	A	B	C	D	E
4.	A	B	C	D	E	14.	A	B	C	D	E
5.	A	B	C	D	E	15.	A	B	C	D	E
6.	A	B	C	D	E	16.	A	B	C	D	E
7.	A	B	C	D	E	17.	A	B	C	D	E
8.	A	B	C	D	E	18.	A	B	C	D	E
9.	A	B	C	D	E	19.	A	B	C	D	E
10.	A	B	C	D	E	20.	A	B	C	D	E

PLEASE PRINT LEGIBLY

LAST NAME	FIRST, MIDDLE NAME		EMPLOYEE/ID NO.
JOB CLASSIFICATION	ITEM NO.	DEPT/DIVISION	P/L
WORKFORCE MEMBER SIGNATURE			DATE
☐ **Check here if non-DHS/non-County Workforce Member**	SCHOOL/EMPLOYER NAME		PHONE NO.

I attest I have read the Privacy & Security Survival Training: Protecting Patient Information Study Guide and am familiar with the contents and will abide by the guidelines set forth.

If I have any questions or concerns, I will talk to my supervisor or the facility Privacy or Information Security Coordinator.

SUPERVISOR/MANAGER NAME (PRINT)	SUPERVISOR/MANAGER SIGNATURE	DATE
Justin Gillenwater		

Distribution: Original - Area File Copy - Facility Human Resources

LAC+USC Healthcare Network Systems Access Application

(* Required fields to be completed, if applicable)

◯ Addition ◯ Deletion ◯ Revision ◯ Move ◯ Reactivate Date: _____

Employee Information:

* First Name: _____ Mi: _____ * Last Name: _____

* Employee #: _____ * SID#: _____ * DOB (mm/dd/yy): _____

* Job Title: _____ ◯ Attending ◉ Fellow ◯ Resident ◯ Intern(PG1) ◯ Medical Student ◯ Midlevel

* Phone #: _____ * Pager #: _____ ◯ County Employee ◯ Contractor

* Department: _____ * NPI#: _____ * Email Address: _____

Building: _____ Room: _____

Are you transferring from another county department? ◯ Yes ◯ No

Applications Needed:

◉ Domain ◯ GroupWise E-Mail ◉ Affinity ◉ Synapse ◉ Quantim ◯ ORSOS ◯ CCIS ◯ Teletracking

◯ WebSphere / HWLA ◯ Network Cabling ◉ Radiology Information System

◯ Other: _____

◉ Desired Affinity User Group: Physician

	Print Name	Signature	Phone Number	Date
* Applicant:				
* Area Supervisor:	Lynda Rivas		323.409.7720	
Local Security Officer:				

** For Office Use Only **

Affinity: _____ ORSOS: _____ Network: _____ QEDM: _____

Please FAX the completed form to the Applications Security Team at (323) 441-8056.

PLEASE CALL IN 2-3 DAYS TO SEE IF ACCESS HAS BEEN ASSIGNED TO YOU (323) 409-2100.

Privacy & Security Survival Training

Protecting Patient Information

Health Services
LOS ANGELES COUNTY

June 1, 2013

INTRODUCTION

A component of the DHS Compliance Program requires you to be trained on the privacy and confidentiality laws and regulations that affect your job. Use this study guide as a resource and feel free to refer to it for situations you may encounter in your workplace. Also your supervisor or your facility Privacy Coordinator or Information Security Coordinator are available to assist you with any concerns you might have.

Not only do you have a duty to comply with the privacy and confidentiality laws, regulations and standards, but you also have a responsibility to take action if you see or suspect possible violations. This study guide provides information about how to report concerns and about your protections against retaliation for good faith reporting of violations.

Who Must Complete Privacy and Confidentiality Training?

Privacy and Confidentiality training is important because it is your responsibility and DHS holds you accountable to adhere to State and Federal laws, departmental and facility policies and procedures and any applicable standards regarding the protection of patient and other confidential information.

All workforce members must complete Privacy & Confidentiality training. Workforce members include: employees (including managers and other supervisors), 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.

Thank you for doing your part to ensure we act responsibly when handling patient, confidential, or sensitive information.

Table of Contents

Learning Objectives

By reviewing the material in this handbook, you will:

- Familiarize yourself with the Patient Privacy & Information Security component of the DHS Compliance Program.

- Learn key elements of HIPAA, the Omnibus Rule, the HITECH Act, California privacy laws, and other relevant laws and regulations.

- Become aware of your responsibility to make sure you do not inappropriately acquire, view, access, use, or disclose patient information and other kinds of confidential information.

- Recognize the importance of safeguarding patient and confidential information.

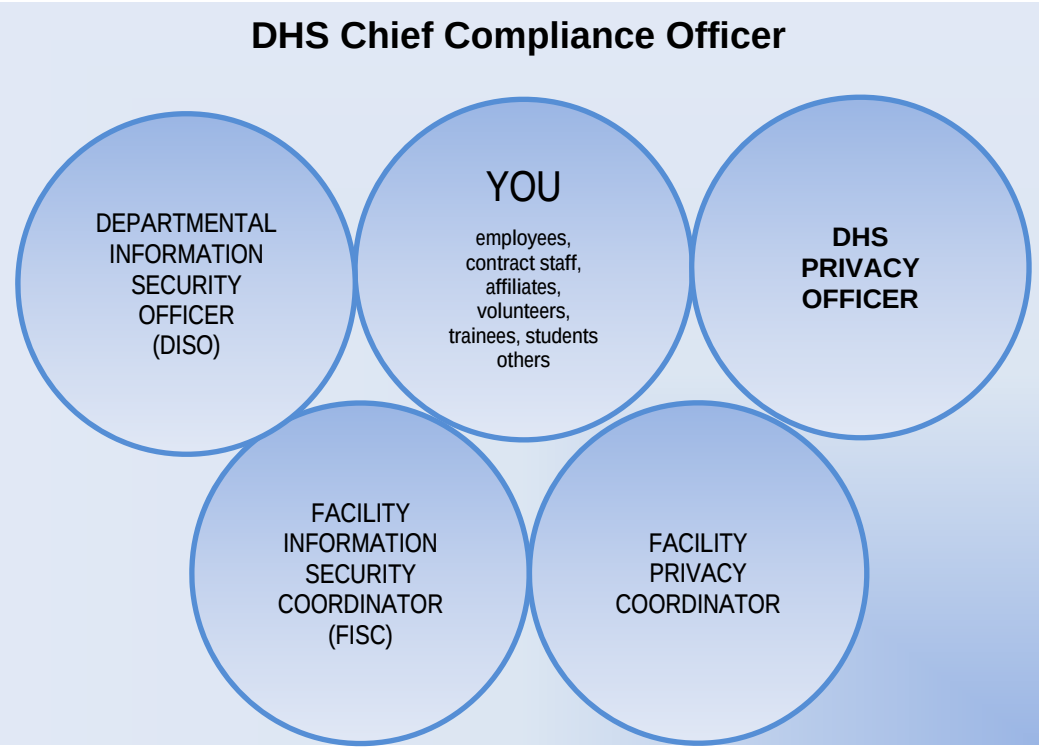
- Learn how to recognize and report suspected privacy and security violations and other compliance issues.

PRIVACY & SECURITY COMPLIANCE PROGRAM

The DHS Privacy & Security Compliance Program is designed to ensure workforce compliance with all applicable laws, regulations, policies and standards that pertain to the privacy and security of patient health and other confidential information. The objectives of this program are:

- Establish and implement policies and procedures to guide the workforce in making good decisions when handling and using patient information.
- Make the workforce aware of their responsibility to assure the privacy and security of patient health information and other confidential or sensitive data and records.
- Provide the workforce with privacy and security awareness training.
- Provide a mechanism for reporting violations and complaints.
- Provide investigative support and oversight of mitigation efforts.

DHS Privacy and Security Program Structure



As a member of DHS' workforce, you may be in contact with patient information and other confidential or sensitive information, records and data in your everyday duties and responsibilities. No matter your job title or function, you are an integral part of the Patient Privacy & Information Security Program and its success depends on you.

The program is comprised of the DHS Privacy Officer, Facility Privacy Coordinator, Facility Information Security Coordinator (FISC), Departmental Information Security Officer (DISO), various committees, and most importantly, **you** as a member of the workforce.

Roles & Responsibilities

Individuals at each facility oversee and coordinate specific responsibilities of the DHS Patient Privacy & Information Security Program.

ROLES	RESPONSIBILITIES
DHS Privacy Officer & DISO	▪ Direct and implement DHS Privacy and Information Security policies and procedures ▪ Direct Privacy and Security Training and Awareness Activities ▪ Ensure compliance with all laws, rules, regulations and standards related to the privacy and security of patient and other confidential or sensitive information
Facility Privacy Coordinator & FISC	▪ Receive, investigate, and report privacy and security complaints or suspected violations ▪ Coordinate the development, implementation and maintenance of specific privacy and security policies and procedures ▪ Monitor the effectiveness of the Patient Privacy & Information Security Program within their facility ▪ Provide facility/area specific training

The name and contact information for the Facility Privacy Coordinator and Information Security Coordinator is listed in your facility orientation/re-orientation handbook.

PATIENT INFORMATION PRIVACY LAWS

HIPAA

The Health Insurance Portability and Accountability Act of 1996 or HIPAA is a federal law designed to protect confidential patient information known as protected health information, or PHI. HIPAA requires DHS' healthcare facilities to institute safeguards to protect patient information. Technological advances in the healthcare industry such as electronic transactions and electronic medical records required changes in law to protect the personal health and financial information contained in those records and to provide patients' rights regarding the use of those records.

HIPAA:

- Provides patients with rights regarding the use and disclosure of their PHI
- Requires DHS and its workforce to take reasonable safeguards to protect the privacy of patient information.
- Requires uses and disclosures of most PHI to be authorized (unless related to treatment, payment, or healthcare operations, or permitted by law or applicable regulation).
- Imposes penalties for violations of the law.

HIPAA has three components: the **Privacy Rule**, the **Security Rule**, and **Transactions and Code Sets**. This study guide focuses on the Privacy and Security Rules. The rules for Transactions and Code Sets govern healthcare transactions, diagnoses and procedure codes, which are covered in specialized unit-based training for workforce members in billing, claims and coding of medical records.

The Privacy Rule protects health information in all forms, including:

- Written
- Oral
- Electronic (ePHI)
- All other forms of communication (e.g., recorded information such as photographs or videos, filming or other recording of patients or PHI).

The Security Rule protects ePHI (electronic protected health information).

THE HIPAA OMNIBUS RULE

The Omnibus Rule (Rule) came about as a result of changes to several federal laws and strengthens the privacy and security protections for health information under HIPAA. The Rule enhances a patient's privacy protections, provides individuals with new rights regarding their personal health information, and strengthens the government's ability to enforce the law. The Rule became effective on March 26, 2013 and DHS must comply with the provisions by September 23, 2013.

The Omnibus related modifications to the Privacy and Security rules include:

- Makes business associates that work with DHS directly liable for compliance with certain HIPAA Privacy and Security Rule requirements.
- Expands a patient's right to receive an electronic copy of their health information.
- Restricts DHS from letting a health plan such as Medicare, Medi-Cal, or an insurance company know about treatment the patient paid for in full out of pocket.
- Requires DHS to make changes to and re-distribute the Notice of Privacy Practices.
- Makes changes to rules that require patient authorizations and other requirements regarding research.
- Makes changes to rules regarding disclosure of child immunization information to schools.
- Makes changes to rules regarding access to decedent information by family members and others.
- Incorporates the increased and tiered civil money penalty structure provided by the HITECH Act.
- Prohibits most health plans from using or disclosing genetic information for underwriting purposes in accordance with the Genetic Information Nondiscrimination Act (GINA).
- Strengthens the limitations on the use and disclosure of protected health information for marketing and fundraising purposes and prohibits the sale of PHI without individual authorization.

HITECH ACT

The Health Information Technology for Economic and Clinical Health Act (HITECH Act) includes additional HIPAA enforcement provisions to ensure the privacy and security of electronic health records.

The HITECH Act:

- Requires notification to U.S. Department of Health and Human Services (HHS) and individuals affected by a breach of unsecured PHI (PHI that was not encrypted, shredded, destroyed, wiped clean or sanitized).
- Provides for additional patient privacy rights
- Prohibits the sale and marketing of PHI
- Increases fines and penalties for violations.
- Strengthens enforcement measures.

State Laws and Regulations

Before the Federal HIPAA law was adopted, California already had patient information privacy laws, such as the Confidentiality of Medical Information Act **(CMIA)**, and the Patient Access to Health Records Act **(PAHRA)**. With the disclosure of several high profile patients' health information, such as in the instances of Maria Shriver (former gubernatorial first lady) and performers Farrah Fawcett and Britney Spears, several new laws were implemented to prevent unauthorized viewing, selling, or disclosure of patient information and to strengthen enforcement measures.

The California Department of Public Health investigates licensed healthcare facilities and programs when alleged privacy breaches are reported and may fine the licensee if determined that unauthorized and/or inappropriate access or viewing of patient medical information without direct need-to-know occurred. Licensed healthcare facilities and programs are obligated to notify the patient and report privacy breaches within five business days from when the breach was detected.

The California Office of Health Information Integrity (Cal OHII) was created to investigate individuals and hold them accountable if they are involved in a privacy breach and can impose fines on the individual for negligent and unlawful disclosures of patient information. They can also report this information to an individual's license, certificate, registration, or permit issuing board or agency for disciplinary action.

While HIPAA and California law generally provide the same protections for patient information, some disclosures of patient information allowed under HIPAA are not allowed under California law. In some cases, California law provides greater patient protections and should be followed.

Regulatory Standards

The Joint Commission (TJC) and Centers for Medicare and Medicaid Services (CMS) standards also require DHS facilities to maintain the privacy and security of patient information. Failure to maintain the confidentiality of patient information can lead to significant fines and can also affect the accreditation and reimbursement for patient care services at our facilities.

Test your knowledge #1 – Violating Patient Privacy
Hospitals and healthcare facilities are responsible for making sure a patient's health information is kept confidential and private. You are a member of the healthcare organization, in what ways can you violate patient privacy? **a.** Inappropriately viewing patient information **b.** Using or disclosing patient information for treatment, payment, or healthcare operations **c.** Encrypting e-mails and sanitizing computer hard drives **d.** Disclosing patient information to business associates ***Answer on page 37***

PATIENT INFORMATION PRIVACY LAWS & RELATED PROCEDURES

This study guide generally describes the key components of HIPAA and DHS' related procedures. DHS' procedures take into account other privacy regulations in addition to HIPAA, including California law and regulatory standards. These non-HIPAA requirements are described herein when they require additional protection of patient information beyond the protections required by HIPAA.

What is Protected Health Information (PHI)?

Protected Health Information can be defined as any health information, created, used, stored, or transmitted by our department that can be used to describe the health and identity of an individual. PHI includes:

- Information that describes the physical or health or condition of an individual.
- Delivery of care services or treatment of an individual.
- Payment for healthcare provided to the patient.

Further, PHI can:

- Be obtained, provided, used, or disclosed during treatment, payment, or approved for healthcare operations.
- Include information related to past, present, or future condition of the patient.
- Be in any form, whether oral, written, or electronic, which can include videos, photographs, and x-rays.

Health Information Identifiers

There are many identifiers that accompany health information that can be used alone, or in combination, to identify an individual. Individually identifiable health information includes any of the following:

- Name
- Address, City, County, Zip code
- Telephone Number
- Medical Record Number
- Social Security Number
- Full-face Photograph
- E-mail Address
- Fax Number
- Date of Birth, Date of Death
- Account Number
- Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the data)
- Certificate or License Number
- Device Identifiers and Serial Numbers
- Internet Protocol (IP) Address
- Health Insurance Beneficiary Numbers
- Vehicle Identifiers and License Plate Number
- Web Uniform Resource Locators (URLs)
- Biometric Identifiers (finger, voice, retinal)
- Certificate or License Number
- Device Identifiers and Serial Numbers
- Genetic Information

Since any one or more of these identifiers could be used to determine the identity of a patient, de-identifying or deleting all such identifiers from a patient's record and any other information which could identify the patient is necessary for the PHI to be considered de-identified. De-identifying or deleting all such identifiers from a patient's records, will limit the amount of information disclosed. Whenever a de-identified record is required, contact the facility Health Information Management (HIM) department.

Where can PHI be Found?

You may come across PHI in many different places, even some that you may not even think about such as labels on prescription bottles, IV solutions and pathology slides. PHI must never be thrown in trash cans. If you find PHI in a trash can, promptly remove it, if safe to do so, or secure the trash can and notify your supervisor.

Listed below are examples of some places where PHI can be found:

- Electronic and hard copy medical records
- Immunization records
- Billing statements
- Faxes
- Reports
- E-mails
- X-rays
- Prescription bottles
- IV solutions
- Diet menus
- Mailings
- Computers
- Portable electronic devices (e.g., USB/flash drive, Smartphone/PDA)
- Patient census and work assignment lists
- Registration forms
- Routing slips
- Diagnostic material and equipment such as pathology slides and patient monitoring equipment

KEY COMPONENTS OF PATIENT INFORMATION PRIVACY LAWS

The key components that will be discussed in this study guide include:

- Patient Rights
- Use and Disclosure of Patient Information with and without Authorization or Opportunity to Object
- Access to PHI
- Minimum Necessary Requirements
- Safeguarding Confidential and Patient Information
- Training
- Privacy & Security Breach Reporting
- Disciplinary Action and Penalties
- DHS Policies

Patient Rights

Under HIPAA, patients have the right to:

Receive a copy of the Notice of Privacy Practices

The Notice of Privacy Practices (NPP) is a document that explains to patients how we may use their health information and to whom we may disclose their information. It describes patient rights regarding their information and how to file a complaint, and provides patients with contact information in case they require additional information.

DHS is required by law to offer patients a Notice of Privacy Practices (NPP) at their first visit to one of our healthcare facilities, and patients are requested to sign an acknowledgment that they received the NPP. This task is generally performed by Patient Financial Services (PFS) staff. If PFS is unable to obtain a signature from the patient (e.g., if first visit was an emergency situation) the reason for not getting the signature should be documented on the form and a signature should be obtained as soon as reasonably possible. Healthcare **must never** be withheld because the patient refuses to sign acknowledgment of the NPP.

All DHS workforce members involved in direct patient care or who have access to PHI are required to be familiar with the terms of the NPP, which is available from your facility Privacy Coordinator or on the DHS website at www.dhs.lacounty.gov.

Access, inspect and request copies of their PHI

With few exceptions, patients have the right to access, inspect and request copies of their PHI. Patients may request paper based or electronic copies of their health information. The Health Information Management (HIM) department in each facility is responsible for providing patients with access and/or copies of their records when the patient has provided written authorization. You must refer all patients requesting access to or copies of their health record to HIM.

Authorize use and disclosure of PHI and request restrictions

Patients may authorize in writing the use of their health information or the disclosure of their information to other persons. Patients also have the right to request restrictions on the use and disclosure of their health information. DHS generally does not have to agree to the restrictions if the use and disclosure does not violate HIPAA or HITECH privacy standards.

Patients have the right to restrict certain disclosures of PHI to a health plan concerning treatment or services for which the patient has paid out of pocket in full.

Parents generally have the right to access their minor child’s medical records except where specific State laws prohibit this right. Minors, 12 years of age and older, have the

right to certain healthcare services and tests without parental consent. Where State law allows minors to consent to treatment or services, parents do not have the right to access those medical records unless authorized by the minor. Refer to DHS Policy 314.1 which describes the specific services that a minor can legally consent to without the need of a parent or legal guardian.

Providers have the right to not disclose information to the parent or a patient's personal representative if he or she believes in their professional judgment that the patient might be a victim of domestic violence, abuse, or neglect. Please note that mandated reporters are required by law to make a formal report of suspected abuse or neglect to appropriate authorities. Refer to DHS Policy 321.001 for further guidance on reporting suspected abuses.

Request confidential communications of their PHI

Patients may request that communications with them be conducted in a particular manner or location to ensure their privacy. For example, a patient may provide an alternative address or personal phone number to receive confidential communications. Such requests must be in writing and are usually granted, if reasonable.

Request amendments or corrections to their healthcare records

Patients may submit a written request asking to amend or make changes to their health records. You must refer the patient and forward any requests to the facility HIM department.

Obtain an accounting of disclosures

Patients may obtain an accounting of disclosures (e.g., a list showing when and to whom the patient's information has been legally shared without their prior authorization) from the facility HIM department.

File a complaint

Patients have the right to file a complaint regarding the use and disclosure of their PHI. All complaints must be promptly investigated. Patients may file a complaint at the facility with the patient advocate or the privacy or information security coordinator in accordance with facility policy and procedure. The patient may also file a complaint with any person or entity indicated in the NPP.

Test your knowledge #2– Patient Rights
Patients have the right to: a. Complain, amend, inspect, and discard their PHI b. Inspect and receive a copy of their PHI, request amendment and restrictions, obtain a list of disclosures, and file a complaint c. Refuse to sign, complain, inspect, destroy, and modify d. Privacy, request disclosures, amend, and destroy ***Answer on page 37***

Use and Disclosure of Patient Information

Use: Accessing or sharing PHI within our department.
Disclosure: Releasing or sharing PHI outside of our department.

There are three types of uses and disclosures:

- Without patient authorization or opportunity to object.
- With patient opportunity to agree or object.
- With patient authorization.

Use and Disclosure without Patient Authorization or Opportunity to Object

HIPAA permits the use and disclosure of patient information without prior patient authorization or an opportunity to object to:

- Provide treatment.
- Administer healthcare payment activities.
- Conduct healthcare operations.
- Other limited and specified instances, such as reporting for public health purposes or when required by law.

Treatment includes activities such as providing healthcare services, ordering medications, and patient referrals.

Healthcare Payment includes activities such as billing, reimbursement for provision of care, collection activities, and other activities related to the reimbursement of providing healthcare.

Healthcare operations are administrative, financial, legal, and quality improvement activities needed to support business operations and maintain quality of care. Such activities include responding to subpoenas/court orders, auditing, and patient registration.

Other limited and specified instances, such as reporting for public health purposes or when required by law - HIPAA also allows the use and disclosure of patient information without patient authorization for other purposes such as State and Federal public health reporting requirements, mandated reports of child, elder, and dependent abuse, and in some instances, for judicial, law enforcement, and governmental oversight activities. Any associated release of patient medical records in these circumstances is the responsibility of the facility's HIM staff, and you must refer all requests to HIM.

Use and Disclosure with Patient Opportunity to Agree or Object

HIPAA permits the following uses and disclosures of patient information when the patient is informed in advance of the use or disclosure and has an opportunity to agree or object:

- Listing patient name, room number, general condition, and religious affiliation in a facility directory.

- Providing patient religious affiliation (and other directory information) to clergy.

The patient must be given the opportunity to agree or object to certain uses or disclosures of their patient information. These uses or disclosures include providing the patient's name, location, general condition, and religious affiliation to persons who request the patient by name or to clergy or listing this information in the facility directory.

Disclosures to Family and Friends

Licensed healthcare providers should use good professional judgment when disclosing information to a patient in the presence of a spouse, family members or friends. It is permissible to disclose health information to:

- Persons identified by a patient, patient's care surrogate, or any other person authorized to make healthcare decisions on behalf of the patient.

- If the patient is present or otherwise available prior to the disclosure, and has the capacity to make healthcare decisions, the provider may discuss the information with family and others.

- If the patient agrees or, when given the opportunity, does not object.

Licensed healthcare providers can share the information if they can reasonably infer, based on professional judgment, that the patient does not object. Limit the shared information to relevant current information. Disclosed information should not contain past diagnoses or conditions not relevant to the current condition; share only what will help with the patient's care and note it in the medical record.

NOTE: If the patient provides a verbal request to disclose or restrict information to certain individuals, note the request in the medical record. When in doubt, always ask the patient.

Use and Disclosure of Patient Information with Authorization

Uses or disclosures of patient information must have the patient's authorization except:

- those related to treatment, payment, or healthcare operations, or
- that do not require the patient to agree or object, or
- are specifically allowed by law, such as a mandated report.

Valid written authorizations must be completed on the DHS "Authorization for Use and Disclosure of Protected Health Information" form. Refer to DHS Policy 361.4 for additional details on the use and completion of the authorization form.

Test your knowledge #3 – Disclosure to Family Members, etc.

Picture this scene: A son is at his mother's bedside. The doctor approaches the bedside.

The doctor says: "Ms. Jefferson, the results of your test indicate that your neurological problems are related to the progression of your HIV positive status."

Did the doctor violate the patient's privacy?

Answer on page 37

Photographing and Recording Patients

Written patient authorization must be obtained prior to taking photographs, video, or audio recordings of patients.

- Authorization must contain the specific reason and use and is only valid for that particular request.

- Only facility-owned cameras, memory cards and other equipment may be used.

- Use of your personal photography or recording equipment (including cellular telephones, smartphones, and other electronic devices) is prohibited.

- DHS Policy 304 provides guidelines for photographing and recording patients.

Incidental Disclosures

Sometimes PHI is disclosed as a by-product of doing business or certain business practices. Incidental disclosures occur when we call out a patient's name in the waiting room or post the patient's name on the wall or door outside their hospital room. These actions are permitted as long as they are a by-product of a permitted use or disclosure, such as for treatment or payment and reasonable steps are made to minimize the amount of information disclosed.

Disclosures to Media

Selling patient information to the media is prohibited and against the law. The media have many ways of gathering information, but it is generally illegal to provide patient information to them without the patient's authorization. You should contact your facility Public Information Officer or the Privacy Coordinator any time the press or news media request information about a patient in one of our facilities.

Unauthorized Disclosure

PHI can only be disclosed to authorized individuals. For example, you may not disclose or provide patient information to:

- Workforce members who are **not** involved in the patient's direct treatment or who are not part of the patient's healthcare team.

- Third-parties not involved in treatment, payment or healthcare operations.

- Your family, friends, or coworkers.

You are only allowed to view, disclose, or access PHI of patients under your care or if you have been authorized to do so based on your job responsibilities. You may only disclose patient information to persons involved in the patient's direct treatment or are members of their healthcare team. If your family member or a personal friend is admitted to the hospital, you do not have the right to view or disclose information about that individual. Do not access or view medical information of coworkers, nor provide information to coworkers upon their request. It is natural for family members and friends to be concerned about their loved one's condition, but it is against the law to access those records without the patient's authorization except as explained previously.

In addition, you should not access your own medical record but follow DHS policy in order to request access to your medical record.

Talk to your supervisor if you feel pressured to provide PHI to someone you feel is not authorized to receive it or if you have questions about the disclosure of information.

Social Networking Sites

Do not post information about patients or work-related issues on social networking sites such as Facebook, MySpace, Twitter, YouTube, etc. Although these sites can be accessed during your scheduled time off from your own personal computing device (e.g., computer, mobile phone, laptop, etc.), you should remember that due to the nature of your work and the type of business you work in, just small bits of information, put together, can reveal identifying information about patients and cause you to violate privacy laws.

Test your knowledge #4 – Social Network Sites

Scene: A man is shot outside of the hospital and comes into the hospital for assistance. Hospital workers go home and talk about the incident on a social networking site.

Hospital worker: "Today was a bear. This guy came into our facility with a gunshot to the head. I don't know how he was walking but he must have had a lot of adrenaline 'cause he really tore up the place asking for help. I had to go downstairs to help clean up the mess."

Friend 1: "That was the guy they showed on TV, right?"

Friend 2: "I saw him come in. He was scary. I was the one who called security."

Friend 1: "They said his name was Harold something?"

Is this an appropriate conversation on a social networking site? Why or why not?

Answer on page 37

Access to PHI

In order to access PHI, you must have a legal or business "need-to-know."

Your job responsibilities determine how much access and the level of access you can have to patient information. Your supervisor will arrange for you to obtain access to systems and networks necessary for you to fulfill your job duties.

- If you acquire, view, use, or access, patient information not related to your job or inappropriately disclose patient information, you will be in violation of DHS policies, HIPAA, and/or State law and may be subject to disciplinary action, criminal and/or civil penalties, and/or imprisonment.

- If your job responsibilities require you to have a license, certification, registration, or permit, you may also be reported to the issuing agency or board and subject to additional disciplinary actions.

Minimum Necessary Requirements

- Under the HIPAA Privacy Rule, workforce members may only access the minimum information necessary to do their job. The purpose and the role of the individual requesting information will determine how much information is allowed to be disclosed.

    - **Example:** Elaine is the nurse assigned to care for Mr. Garcia; in order to make sure he is receiving the right treatment she needs to have access to his entire medical record. In contrast, Hector, is a registration clerk, he only needs the basic demographic information about the patient, not the treatment record.

- Minimum necessary applies to most uses and disclosures of PHI, but this standard does not apply to uses or disclosures related to direct treatment of the patient or to certain other specific requests.

All releases or disclosure to outside agencies, to the patient, or not required for treatment, payment, or healthcare operations must be done through the facility's HIM department.

Inappropriate Access

- It is **never** acceptable for you to look at confidential or patient information "just out of curiosity," even if no harm is intended.

- It does not matter whether the information pertains to a celebrity, political figure, or other "high profile" person, fellow workforce member, a close friend, family member, or yourself.

You must protect and keep private **ALL** patient information, no matter whose it is.

Just because you have access to a system or network or patient records, does not mean you have the right or authorization to access or view confidential or patient information that does not pertain to your job. All patient information is confidential and must be protected at all times.

Unauthorized Access

- Unauthorized access to networks or systems containing PHI or other confidential information includes:
    - Access without authorization.
    - Using someone else's password and/or user ID.
    - Letting someone else log you into the network using their password.
    - Giving someone your password to log into the network.
    - Using your password to log someone else into the network.
    - Accessing information without a job-related "need-to-know."
- You are responsible and will be held accountable for all access to networks or systems using your password.
- Be wise and only access systems and data as authorized.

Test your Knowledge #5 – Inappropriate Access

Scene: A workforce member is talking to her coworker.

Clerk: Guess who I just saw being treated in the clinic downstairs?

Coworker: Who?

Clerk: It was TH, the guy who works in information systems!

Coworker: I wonder what's wrong with him?

Clerk: Let's see if I can find him in the electronic health information system so we can find out. I'll keep you posted!

Will the clerk violate the patient's privacy?

Answer on page 38

DHS PRIVACY AND INFORMATION TECHNOLOGY (IT) SECURITY POLICIES

You are required to review and comply with the relevant privacy and IT security policies, including:

- Acceptable Use Policy for County Information Technology Resources (DHS Policy 935.20)

- Safeguards for Protected Health Information (DHS Policy 361.23)

You are provided with these policies for acknowledgment during in-processing. These policies must also be reviewed each year as part of your Performance Evaluation. You are required to sign an agreement to abide by them.

Acceptable Use Policy

- The County's information technology resources are the property of the County and are to be used for authorized business purposes only.

- You are responsible for protecting all information created using County resources and your access is a privilege that may be modified or revoked at any time for abuse or misuse.

- DHS may log, review, or monitor any data you have created, stored, accessed, sent, or received, and these activities may be subject to audit.

SAFEGUARDS

Safeguards are actions that are taken to protect confidential information from accidental or intentional unauthorized viewing, acquisition, access, use, or disclosure. They can include administrative, physical, and technological steps to reduce the risk of improper access, use, or disclosure of PHI.

Administrative Safeguards

Include the development of policies and procedures, providing privacy and security training, the development and implementation of a complaint and reporting process, and disciplinary actions for violations.

Physical Safeguards

Include securing buildings and equipment, as well as activities such as locking paper medical records in file cabinets or rooms, shredding paper records, and ensuring all exterior doors to buildings, other than designated entrances and exits are locked at all times.

Examples of Physical Safeguards:

- Placing computers, copiers, and fax machines so they cannot be accessed or viewed by unauthorized persons.
- Protecting computers and other electronic media and devices against theft or unauthorized access.
- Maintaining servers and mainframes in a secure area where physical access is controlled.
- Ensuring that all areas used to store PHI are properly secured and allow only authorized personnel to have access.
- Limiting physical access to view or retrieve medical records or other patient information to authorized users.
- Ensuring windows, all exterior doors, other than designated entrances and exits, and other building access points are secured or locked at all times.

Technical Safeguards

Protect PHI maintained in electronic form:

- Always lock (press Ctrl-Alt-Del and select “Lock Workstation”) or log off when you leave the computer even if it is for a short period of time.
- Require computers and other electronic devices to have a password-protected screen saver or other time-out feature.
- Use strong passwords with at least 8 characters, such as a combination of upper/lower case letters, numbers, and/or special characters.
- Keep computer passwords confidential, and do not leave them where they can be seen or accessed.
- Do not use your password to provide access to another user.

- Frequently change your password.
- Be aware of your departmental system downtime procedure, should any automated systems such as patient care or billing become unavailable.
- Laptops, thumbdrives, and other electronic devices containing PHI must be encrypted.
- Keep electronic records related to patients, such as lab reports, correspondence, and other patient or confidential information out of publicly accessible areas or any place where it might be thrown in the trash.
- Exercise caution when unauthorized persons are visiting or completing a temporary assignment in the workplace to protect PHI from inadvertently being viewed. Use caution to avoid inadvertently allowing access or viewing to individuals who do not have a business need to know.

Test your knowledge #6 - Physical Safeguards

Part of your assignment requires you to deliver patient charts to buildings on the campus that are located outside the clinic. The entrance to one of the buildings is located just outside the door which is an emergency exit and is locked at all times.

To avoid having to walk through the clinic to the designated exit and then back around the building, you decide to use the emergency door. Since the door is kept locked, you put a wedge in the door to keep it open so you can get back in after you've made your delivery.

Is this ok? Why or why not?

Answer on page 38

Test your knowledge #7 – Technical Safeguards

Scene: A workforce member is talking to a coworker

WFM: Hi Jim, I've been calling Information Systems to reactivate my account but they're so busy they can't get to me for another few days. Will you log in for me with your user name and password so I can get this high-priority assignment done?

Coworker: Sure, let me do that for you right now. Just make sure to log off when you're done with your assignment.

What is wrong with this scenario?

Answer on page 38

POLICIES FOR SAFEGUARDING PHI

Safeguarding confidential or patient information is your responsibility. The policies described below must be followed to help safeguard confidential and patient information.

Faxing PHI

- If you need to fax confidential or patient information, you must indicate on the fax that it is confidential (Use the fax cover sheet established by your facility.).
- Call and advise the receiving party when the fax is ready to send and ask the individual to confirm receipt.
- Use pre-programmed fax numbers as much as possible.
- If the fax is sent to the wrong person by mistake, immediately inform your supervisor.
- Misdirected faxes sent outside the facility must be investigated and reported to the facility Privacy Coordinator.

If you receive a misdirected fax indicating it contains confidential information, do not read through it. Contact the sender and advise that you received the fax in error and destroy the information.

E-mailing Patient, Confidential, or Sensitive Information

All e-mail communications containing patient, confidential, and/or sensitive information to someone outside of the County's e-mail system must be encrypted to comply with State and federal privacy laws and DHS policies. *E-mail addresses outside of the County's e-mail system that **do not** end with ".lacounty.gov." as for example: @dpss.lacounty.gov, @dmh.lacounty.gov, @ph.lacounty.gov, etc.*

- There must be a business need.
- You must have **specific authorization** from your supervisor to send encrypted e-mails containing patient, confidential, and/or sensitive information.
- Once you are authorized by your supervisor, you must contact your local IT Help Desk to be added to the e-mail encryption solution group. Must comply with the Minimum Necessary Requirements.

- Send the recipient an un-encrypted e-mail notifying them they will be receiving an encrypted e-mail and instructions on how to open it.

- Once you have been authorized and added to the e-mail encryption solution group, then you will have the ability to send a secure e-mail. You must add the word “Secure” in square brackets **[Secure]** in the subject line of the e-mail.

Incoming e-mail containing ePHI, confidential, or sensitive information must be kept secure.

E-mail must not be used for urgent communications; it may be used as follow-up after a phone call to document the discussion.

Safeguarding in Public Areas

Exercise care when discussing or providing patient information:

- Use lowered voices.

- Do not talk about patient care in public areas like elevators, the cafeteria, or public transportation.

- In joint treatment areas, be mindful of what you say even when the curtain is closed.

- Be careful when leaving a voice mail message.

- On public transportation, make sure you use a security screen on your laptop, and keep paper materials out of public view.

Test your knowledge #8 – Safeguarding PHI

Three patients are in a joint treatment area of an emergency room, each in bed and separated by partially drawn curtains. A physician enters the room with a medical chart.

Doctor: Ms. Johnson?

Patient in middle bed: Yes, that's me.

Doctor (in a normal speaking voice, with curtains open): Ms. Johnson, your lab results have come back and you have been diagnosed with cirrhosis of the liver.

Ms. Johnson: Oh my gosh, what does this mean?

Doctor: Well Ms. Johnson, this means that you have a scarred liver as a result of your chronic alcoholism.

Question: Name four actions that can be done to comply with the HIPAA Privacy Rule and protect the patient's privacy?

Answer on page 38

Test your knowledge #9 – Leaving phone messages

1. Nurse: Good Afternoon, this is Walter from the Oncology Department at Franklin Hospital, calling to remind you of your cancer screening follow-up appointment for Wednesday, August 16 at 9:00 a.m. Please call me at 505-555-1216, if you need to reschedule.

2. Nurse: Hello, this is Connie from Franklin Hospital, calling to remind you of your appointment on Thursday, July 14th at 3:00 p.m. Please call 505-555-1216, if you need to re-schedule.

Did the nurses leave appropriate phone messages?

Answer on page 38

Storing and Saving ePHI

All portable devices (e.g. laptops, USB thumb drives, external hard drives, etc.), whether or not the devices are owned or provided by the County, used for County business and/or contain patient, confidential, or sensitive information must be encrypted.

Laptops:

An encrypted laptop can be identified visually by:

- A red sticker with the word “Encrypted” tagged on the upper right-hand corner of the laptop lid.
- A grayed-out “P” in the bottom right corner of the screen if you are running Windows XP or a yellow padlock if you are running Windows 7.
- You must contact your local IT Help Desk for encryption support if you are unable to identify and/or confirm that the laptop is encrypted.

Portable USB Storage Devices (thumbdrives)

- Use of portable USB storage devices is limited to authorized individuals.
- The device must be encrypted if storing PHI. Password protecting a file or thumbdrive DOES NOT meet the encryption requirement.

Computer Security

Do not store or save patient information on the computer’s hard drive or on a removable drive. All patient information must be stored or saved on the network drives.

You must log off or lock any computer system/terminal when you leave the computer station or after you have obtained the necessary data.

- To log off, press Ctrl-Alt-Del and select “Log Off.”
- To lock, press Ctrl-Alt-Del and select “Lock Workstation.”

Destroying PHI

Properly dispose of patient information. Shred hardcopy documents that contain PHI or place them in a locked shredder bin. NEVER throw PHI in the trash, recycle or use it for scratch paper.

If you discover PHI that has not been disposed of properly, such as thrown in a trash can, remove it from the trash can, if safe to do so, or secure the trash can and immediately notify your supervisor.

Contact your IT/Help Desk to appropriately destroy ePHI located on electronic media (e.g., CD's, USB thumb drives, hard drives, etc.).

Remember

- Do not leave confidential or patient information unattended or in a place where others can see it.

- Avoid using sticky notes, scratch paper, notebooks, etc. to record patient information; if you must temporarily record information in this manner, promptly and properly destroy the information.

- Use of patient whiteboards must be restricted to areas where the information cannot be seen by unauthorized persons.

- Patient sign-in sheets should only contain limited information such as name, date, and time. They should not contain the reason for the visit.

- Fax machines should be in secure areas.

- Contact the facility HIM department for release of patient information to the patient and to outside agencies, including law enforcement.

- If you see or hear about a violation of patient confidentiality, it is your responsibility to report it.

PRIVACY AND SECURITY BREACH REPORTING

Privacy breach and/or security breach is the term we use for the attempted or successful unauthorized viewing, access, use, disclosure, or destruction of patient information. This term includes a variety of activities prohibited under State and Federal law.

California law prohibits the unauthorized access to, and use and disclosure of, a patient's medical information. Inappropriately accessing and viewing such information without a direct "need to know" that information is a violation of this law.

> ***For example***, if a workforce member peeks at a patient's medical record for the sake of curiosity, it is reportable to the State even if the information was not shared with another person or there was no proof of patient harm. State law requires notification of all breaches within five (5) business days to the patient and the California Department of Public Health.

The HIPAA Omnibus Rule defines a **breach of unsecured PHI** as the unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of the PHI. The Rule requires us to notify the U.S. Department of Health and Human Services regarding a breach of unsecured PHI unless we can demonstrate that there is a low probability that the PHI has been compromised. To demonstrate that there is a low probability that a breach compromised PHI, DHS or the involved business associate must perform a risk assessment that addresses at minimum the following factors:

- The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification.
- The unauthorized person who used the protected health information or to whom the disclosure was made.
- Whether the protected health information was actually acquired or viewed.
- The extent to which the risk to the protected health information has been mitigated.

If a breach has occurred, the person whose information was breached must be notified. Also, if the breach involves 500 or more individuals, not only does the breach need to be reported to the U.S. Department of Health and Human Services but also broadcast in a popular news outlet. In some cases, notification of the breach will also be posted on the DHS and facility websites.

HIPAA also refers to computer **security incidents**. A computer security incident is the attempted or successful unauthorized viewing, access, use, disclosure, or destruction of information. Examples of security incidents include looking at files without a business need, using someone else's password, providing your password to someone else, using your password to log into a system for someone, sharing confidential information without authorization, and deliberately misplacing files. Security incidents also include interference with information system operations, such as hacking into electronic systems, computer theft, or unauthorized alteration or destruction of electronic information/equipment. Security incidents include many incidents that do not rise to the level of being a breach

Test your knowledge #10 – Security Breaches
Elizabeth, an employee, heard that her granddaughter was a patient at the hospital and decided to look her up in the clinical information system. Is this a reportable incident? ***Answer on page 38***

Reporting Privacy and/or Security Breaches

Any and all suspected and actual privacy breaches and/or security breaches must be immediately reported to your supervisor, facility Privacy Coordinator, and/or facility Help Desk.

- It is your responsibility to report any activity that appears to violate privacy or security laws, rules, regulations, or policies.
- There will be no retaliation if you report a suspected or actual violation in good faith.
- Any workforce member who knowingly makes a false accusation may be subject to discipline.
- Reporting a violation does not protect you from appropriate disciplinary action regarding your own misconduct.
- Failure to report a violation may subject you to disciplinary action as well as possible civil and/or criminal penalties.

You may also make a report or refer privacy related questions to your facility Privacy Coordinator or:

DHS Compliance Hotline: 800-711-5366

Los Angeles County Fraud Hotline: 800-544-6861

Security related questions may be reported to:

DHS IT Security Compliance Division at **SecurityCompliance@dhs.lacounty.gov**

Test your knowledge #11 – Computer Incident
Michael, an admitting clerk, was showing his friend Hector, a nurse from the cardiac unit, how the electronic medical record system at his hospital worked. While looking at a patient record, he hit a wrong key and accidentally deleted the record from the system. Is this a reportable security incident? ***Answer on page 39***

DISCIPLINARY ACTIONS AND PENALTIES

Remember, **YOU** are responsible and will be held accountable for the privacy and security of confidential or patient information that you acquire, view, access, use, disclose, maintain, or transmit.

Disciplinary Actions

Disciplinary action, **up to and including discharge**, will be imposed for violation of DHS policies and procedures, Federal and/or State laws regarding privacy of information.

Disciplinary actions are progressive and commensurate with the severity, frequency, and intent of the violation(s). DHS applies disciplinary actions equitably without regard to role or position.

Civil and Criminal Penalties

Violations may not only result in disciplinary action, but could result in civil and/or criminal penalties against and/or prosecution of the workforce member.

State Attorneys General also may bring a civil action on behalf of residents of a state for HIPAA violations.

HIPAA Civil and Criminal Penalties

Civil Penalties

Civil penalties can be imposed on facilities for various degrees of HIPAA violations.

Type of Offense	Penalty (per violation)	Annual Penalty Cap for Identical Violations
No actual knowledge of violation (and exercised reasonable diligence)	$100 - $50,000	$1.5 million
Violation due to reasonable cause	$1,000 - $50,000	$1.5 million
Willful neglect with correction	$10,000 - $50,000	$1.5 million
Willful neglect without correction	$50,000 (or more)	$1.5 million

Criminal Penalties

Individuals can be fined and imprisoned for various degrees of HIPAA violations.

- Intentional inappropriate use: up to $50,000 and/or up to 1 year in prison
- Under false pretenses: up to $100,000 and/or up to 5 years in prison
- Malicious harm/commercial or personal gain: up to $250,000 and/or up to 10 years in prison

Any person, not just employees, who accesses, obtains, or discloses patient information without authorization can be imprisoned for up to ten years and fined up to $250,000.

State Civil and Criminal Penalties

Facilities may be fined:
Up to $25,000 per patient and up to $17,500 per subsequent breach of the same patient medical record, plus $100 for each day that the violation is not reported, up to a combined total of $250,000.

Individual providers and workforce members may be fined or assessed penalties as shown in the table:

Type of Offense	Penalty per violation
Negligent disclosure	Up to $2,500
Knowing and willful access, disclosure and use	Up to $25,000
Knowing and willful access and use for financial gain	Up to $250,000
Anyone not permitted to receive medical information who knowing and willfully obtains, discloses or uses it without patient authorization	Up to $250,000

CONSEQUENCES FOR POOR JUDGMENT

Every day there are instances of healthcare facilities and employees who are investigated or convicted of inappropriately accessing or disclosing patient information. A few instances in our own backyard include:

"Octomom" and Kaiser Permanente
Hospital was fined $487,000.
Employees were investigated and terminated, and they may be individually prosecuted or fined.

UCLA Medical Center
California privacy laws were strengthened as a result of the UCLA incident in which an employee disclosed information regarding its famous patients to the media. UCLA agreed to pay a $865,000 fine for the breach. Also, in another case, a former UCLA physician became the first person in California to be indicted and sentenced to four (4) months in prison and fined $2,000 for just snooping into a patient record.

In each of these cases, employees inappropriately accessed a high profile patient's health information, and, in some cases, disclosed and/or sold the information to the media.

CONCLUSION

Protecting patient information is an individual and collective responsibility!

Ask yourself these questions:

- Do I have access to confidential and/or patient information?
- Do I work in an area where confidential or patient information can be viewed by unauthorized individuals?
- What can I do to ensure that I am consistently taking personal responsibility for protecting confidential and patient information?

You must:

- Think about protecting patient information at all times.
- Keep passwords in a safe place and don't share them or sign someone on the network/computer using your password.
- Obtain authorization to send e-mail containing PHI and ensure such e-mails are encrypted.
- Obtain permission to use external drives such as thumbdrives to store PHI. Thumbdrives, laptops, computers and other electronic equipment must be encrypted. (Remember, simply using a password **DOES NOT** meet the encryption requirement.)
- Make sure information you discuss at home and on social media websites do not present a confidentiality or privacy concern to our workplace or for the patients we serve.
- Refer requests for patient medical information to the facility HIM department.
- Report anything that you see or hear that may be a violation of patient information privacy. Report IT! It's Your Responsibility.

If you have any questions regarding the privacy or security of patient information, ask your supervisor or facility Privacy or Information Security Coordinators.

TEST YOUR KNOWLEDGE ANSWERS

Test your Knowledge #1
Answer:
a

Test your Knowledge#2
Answer:
b

Test your Knowledge #3
Answer:

It depends on whether the doctor:

1) Knows the person is involved in the patient's care or is familiar with the relationship;
2) Has given the patient an opportunity to object, and the patient did not; or
3) Has the patient's permission.

Providers should exercise good professional judgment when disclosing patient information in the presence of the patient's family members, spouse, or friends. If in doubt, the provider should ask the patient prior to disclosing the information.

Test your Knowledge #4
Answer:

No, this is not an appropriate conversation to have on a social networking site. Although workforce members should feel free to engage in conversations on social networking sites at home, they should not discuss events or information involving patients or patient information on those sites. Disclosure of patient information may result in:

- Damage to the patient's reputation and/or finances
- Severe liability penalties and fines for the department
- Criminal/civil penalties and fines for the workforce member, including jail time
- Disciplinary actions against a workforce member's license, certification, registration, permit
- Disciplinary action against the workforce member, including discharge or termination

Test your Knowledge #5
Answer:

Yes. Because she does not have a direct treatment relationship with the patient and she does not have a legal right to know, she has no authority to access the patient's PHI.

Test your Knowledge #6
Answer:

This action is a security violation because propping a door open can potentially leave medical records and computer equipment susceptible to unauthorized access and environmental hazards, such as fire.

Test your Knowledge #7
Answer:

While the dedication to work shown by the workforce member deserves praise, logging onto a computer for someone else is the same as sharing a password, which is in violation of the County's HIPAA and Acceptable Use Policies. The workforce member should notify his/her supervisor, who should contact the local IT help desk to resolve the issue.

Test your Knowledge #8
Answer:

1. Close curtain
2. Speak in lowered voice
3. Check ID wrist band to verify identity
4. Minimize use of patient name whenever possible

Test your Knowledge #9
Answer:

No, Walter provided more than the minimum necessary information on the phone, such as specific unit of the hospital or clinic and the purpose of the visit. In the second message, Connie left an appropriate message.

Test your Knowledge #10
Answer:

Yes. Even if she looked at the medical record just for the sake of curiosity, or out of concern, this action would be reportable to the State and the patient, even if the information was not shared with another person, or there was no proof of patient harm.

Test your Knowledge #11
Answer:

Yes, for the following reasons:

- Michael had no business reason to look at the patient's record;
- Showing Hector the record was wrong because he has no business reason to see the information;
- The activity is considered an unauthorized use of patient information; and
- Michael mistakenly deleted PHI from the medical record system.

Special thanks to the following individuals for their resilient dedication and support in the development of the on-line training and this handbook:

Jennifer Papp. R.D.	Privacy Office, DHS
Brenda Booth-West	Privacy Office, DHS
Latonya Calloway	Human Resources, DHS
Sally Foong	Information Systems, DHS
Susan Perez-Amador	Organizational Development and Training, DPH
Talib Hasan	MLK, Jr. Multi-Service Ambulatory Care Center
Betsy Swanson-Hollinger	Organizational Development and Training, DPH
Azar Kattan	Olive View Medical Center
Alma Smith, R.H.I.T.	Harbor-UCLA Medical Center
Raub Mathias	Office of Managed Care

PRIVACY & SECURITY SURVIVAL TRAINING: PROTECTING PATIENT PRIVACY
ASSESSMENT QUESTIONS

1. As a workforce member of this facility, you may access a patient's protected health information:

   a. whenever you want to do so
   b. if your co-worker or supervisor asks you to do so
   c. only if your job duties require you to do so
   d. in an emergency even if you're not authorized

2. It is your responsibility to immediately report any suspected privacy or security breach, such as any theft of computer equipment or unauthorized or inappropriate access, use, disclosure, or destruction of patient or confidential information:

   a. True
   b. False

3. Patient or confidential information should not be viewed, accessed, or disclosed without a need to know. Which of the following forms of confidential information would be protected under HIPAA?

   a. A paper-to-paper fax
   b. Verbal conversations
   c. Information written solely on paper
   d. All of the above

4. You only need to contact your facility Information Technology Help Desk to obtain authorization to e-mail PHI.

   a. True
   b. False

5. If you are only going to be away from your desk for a few minutes you do not need to lock or log off your workstation.

   a. True
   b. False

6. Jason's supervisor wants access to his computer when he is away from the office. The supervisor has a right to know his username and password.

   a. True
   b. False

7. DHS may log, review, or monitor any data you have created, stored, sent, or received using County Information Systems (e.g., computer, laptop, etc.).

   a. True
   b. False

8. What is the Notice of Privacy Practices (NPP)?

   a. It is a tool to enable patients to express their concerns about misuse of PHI
   b. It informs the patient of services the facility does not provide
   c. It is a tool that allows patients to select the type of information that they would like to have sent back to their provider
   d. It describes patient rights and the provider's responsibilities regarding PHI

9. Which of the following are authorized to release patient information when requested by a patient, law enforcement, etc.?

   a. Physicians
   b. Nursing staff
   c. Health Information Management staff
   d. Employee Health Services staff

10. A password on a portable storage device is sufficient to protect PHI in case of loss or theft of the device.

    a. True
    b. False

11. Which of the following disclosures of PHI is *not* a privacy breach and/or security breach?

    a. Mary has access to the patient information system and decides to check her health records to see what is in it
    b. Walter works in HIM and provided a patient's medical information to the United States Department of Health and Human Services
    c. Janice, a law enforcement officer, is friends with the hospital receptionist and asks her to look up her ex-husband's records to check which medicines were prescribed at his last visit
    d. All are allowable under HIPAA

12. Mary has been out sick. Her supervisor finds out from their Human Resources Return-to-Work Unit that Mary has cancer, and tells Mary's coworkers about it. It is okay for Mary's supervisor to let her coworkers know about Mary's cancer since the coworkers all care about her well-being.

    a. True
    b. False

13. You may be subject to fines and penalties under State and federal laws and/or disciplinary action if you fail to comply with patient privacy laws or County, DHS, or facility policies and procedures.

    a. True
    b. False

14. If the State determines you have violated the State privacy laws, they may report you to the appropriate licensing, registration, certification, or permit board/agency for possible disciplinary action.

    a. True
    b. False

15. A patient or individual can report a suspected privacy or security breach to the following entities:

    a. Supervisor
    b. Facility Privacy Coordinator or Information Security Coordinator
    c. County Fraud Hotline
    d. DHS Compliance Hotline
    e. Any of the above

16. There will be no retaliation against a workforce member who, in good faith, reports any actual or suspected privacy breaches or HIPAA violation

    a. True
    b. False

17. In addition to medical records, PHI may be found in written communications, electronic forms, verbal conversations, e-mails and memos, IV and medication labels, X-rays, monitors, EKGs, etc. and must be protected.

    a. True
    b. False

18. While working the 9pm – 6am shift at the hospital, you see some patient information in a trash can. What should you do?

    a. Remove it from the trash can, if safe to do so, and take it to the shredder bin.
    b. Remove it from the trash can, if safe to do so, or secure the trash can and immediately notify your supervisor.
    c. Immediately report it to the facility Chief Financial Officer
    d. Call the toll-free hotline and report it

19. An employee mistakenly receives a fax containing PHI from an outside healthcare agency. What should the employee do?

    a. Contact the person on the cover sheet
    b. Throw the FAX in the shredder bin
    c. Contact the facility Privacy Officer
    d. All of the above

20. When you have a patient's prior written permission to videotape them, it is permissible to use your own video camera.

    a. True
    b. False

Health Services
LOS ANGELES COUNTY

PRIVACY & SECURITY SURVIVAL TRAINING: PROTECTING PATIENT PRIVACY

ANSWER SHEET AND PROOF OF COMPLETION

Instructions: Please circle the correct letter corresponding with the questions in the study guide. You must score 20 correct to receive credit for Mandatory Training.

1.	A	B	C	D	E	11.	A	B	C	D	E
2.	A	B	C	D	E	12.	A	B	C	D	E
3.	A	B	C	D	E	13.	A	B	C	D	E
4.	A	B	C	D	E	14.	A	B	C	D	E
5.	A	B	C	D	E	15.	A	B	C	D	E
6.	A	B	C	D	E	16.	A	B	C	D	E
7.	A	B	C	D	E	17.	A	B	C	D	E
8.	A	B	C	D	E	18.	A	B	C	D	E
9.	A	B	C	D	E	19.	A	B	C	D	E
10.	A	B	C	D	E	20.	A	B	C	D	E

PLEASE PRINT LEGIBLY

LAST NAME	FIRST, MIDDLE NAME		EMPLOYEE/ID NO.
JOB CLASSIFICATION	ITEM NO.	DEPT/DIVISION	P/L
WORKFORCE MEMBER SIGNATURE			DATE
☐ **Check here if non-DHS/non-County Workforce Member**	SCHOOL/EMPLOYER NAME		PHONE NO.

I attest I have read the Privacy & Security Survival Training: Protecting Patient Privacy Study Guide and am familiar with the contents and will abide by the guidelines set forth.

If I have any questions or concerns, I will talk to my supervisor or the facility Privacy or Information Security Coordinator**.**

SUPERVISOR/MANAGER NAME (PRINT)	SUPERVISOR/MANAGER SIGNATURE	DATE
Justin Gillenwater		

Distribution: Original - Area File Copy - Facility Human Resources