Privacy & Security Survival Training

Protecting Patient Information

June 1, 2013

Health Services
LOS ANGELES COUNTY

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:

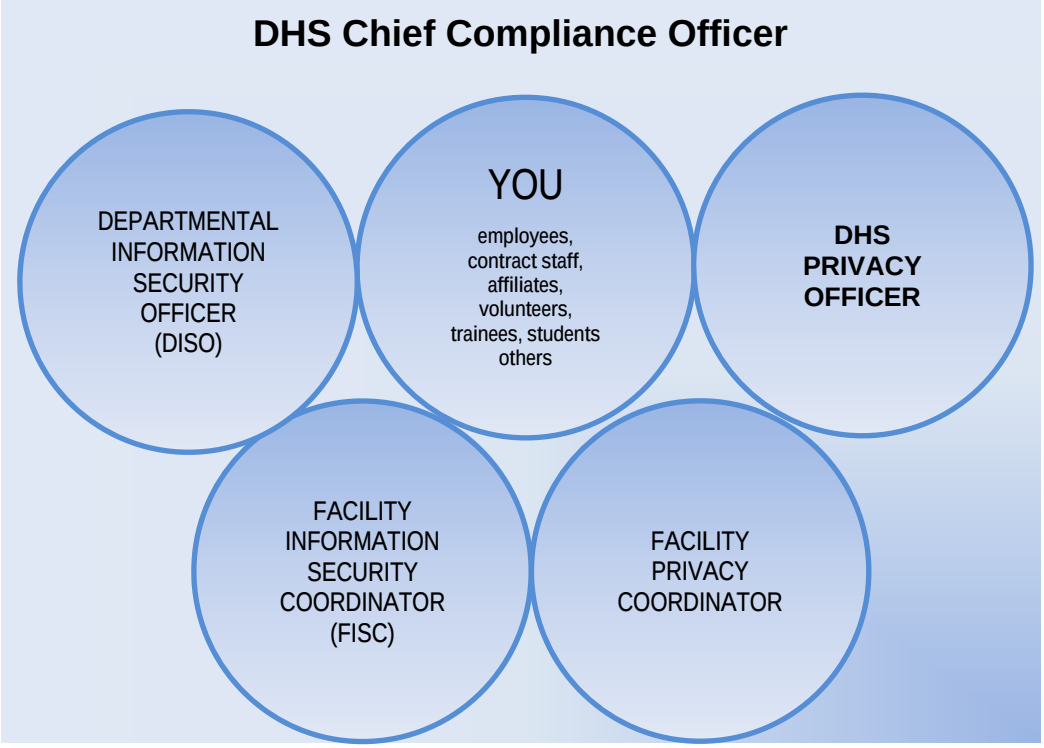
- Familiarize yourself with the Patient Privacy & Information Security component of the DHS Compliance Program.
- Learn key elements of HIPAA, the Omnibus Rule, the HITECH Act, California privacy laws, and other relevant laws and regulations.
- Become aware of your responsibility to make sure you do 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 INFORMATION
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 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

Distribution: Original - Area File Copy - Facility Human Resources

Health Services
LOS ANGELES COUNTY

POLICIES AND PROCEDURES

SUBJECT: DISCIPLINARY ACTIONS FOR FAILURE TO COMPLY WITH PRIVACY POLICIES AND PROCEDURES

POLICY NO: 361.10

PURPOSE:

To state the General Policy of the Los Angeles County Department of Health Services (DHS) related to the unauthorized acquisition, viewing, access, use and/or disclosure of Protected Health Information under the Privacy Standards of the Health Insurance Portability and Accountability Act of 1996, 45 C.F.R. Parts 160 and 164 ("HIPAA Privacy Standards"), and the Los Angeles County and DHS policies and procedures which implement HIPAA ("HIPAA Implementing Policies and Procedures.")

POLICY:

Each DHS facility is required to investigate failures to comply with policies related to Protected Health Information (PHI) privacy, confidentiality, and security, and must impose appropriate disciplinary actions where indicated.

Disciplinary actions are progressive and commensurate with the severity, frequency, and intent of violations. DHS applies disciplinary action equitably without regard to job classification, role or position.

Unauthorized acquisition, viewing, access, use, and/or disclosure of protected health information, or the failure to maintain and safeguard PHI is subject to disciplinary action, including, but not limited to, verbal counseling, written warning, reprimand, suspension, and discharge, in accordance with the provisions of Los Angeles County Civil Service rules, DHS Discipline Manual and Guidelines, and DHS Policy No. 747, "Disciplinary Action."

Disciplinary action will not be applied to a workforce member who discloses protected health information (PHI) to a health oversight agency or an attorney while in the process of reporting either an allegation of unlawful conduct by the entity, a violation of professional or clinical standards, or conditions in the entity that endanger patients (whistleblower). Additionally, disciplinary action will not be applied for filing complaints, testifying, participating in investigations, compliance reviews, proceedings or hearings, or for opposing real or perceived unlawful acts or practices that violate patient medical information privacy and security laws, regulations, and DHS policies provided the report is made in good faith.

Health Services
LOS ANGELES COUNTY

NOTICE OF PRIVACY PRACTICES

Effective Date: September 23, 2013

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

WHO WILL FOLLOW THIS NOTICE OF PRIVACY PRACTICES

This Notice of Privacy Practices (Notice) explains the ways the Los Angeles County Department of Health Services (DHS), including all DHS workforce members, such as doctors, nurses, other health care staff, residents, students training at a DHS facility, and volunteers who help with care at a DHS facility, We may use and disclose (provide to others) medical information about you. The Notice also explains your rights regarding the use and disclosure of your medical information.

We are committed to keeping your medical information private. To manage your care, we create a record of the treatment and services you receive at our facilities. This record is needed to provide you with quality care and to comply with certain legal requirements. This Notice applies to all records of the care provided to you in our facilities.

OUR OBLIGATIONS AS TO YOUR HEALTH INFORMATION

The law requires DHS to:

- Keep your medical records and health information, also known as “protected health information," private and secure.
- Give you this Notice which explains your rights and our legal duties with respect to your health information.
- Tell you about our privacy practices and follow the terms of this Notice.
- Notify you if there has been a breach of the privacy of your health information.

YOUR RIGHTS ABOUT YOUR HEALTH INFORMATION

You have the following rights regarding your health information in our records:

Right to See and Ask for a Copy of Your Medical Record – With certain exceptions, such as records considered psychotherapy notes, you have the right to see and get a copy the medical

records we have of your care. To inspect and copy your medical records, you must make your request in writing, to the facility's Health Information Management Release of Information Unit. For your convenience, you may use the *Request for Access to Health Information* form. If you request a copy of your medical record, we may charge a fee for the costs of copying, mailing, or other supplies associated with your request. If we have your health information available electronically, under certain circumstances, you may be able to obtain this information in an electronic format. The *Request for Access to Health Information* form may be obtained from the DHS website: www.dhs.lacounty.gov or by contacting the health facility where you obtain your services.

In some cases, we may deny your request. In these instances, we will give you the reason for the denial and, with some exceptions, you may request a review of this decision. If you request a review, another licensed health care provider within a DHS facility, who was not involved in the original decision to deny your request, will review the decision. We will follow what he or she decides in the review.

Right to Request Changes (Amendment) Your Health Information – If you feel that the health information contained in your medical record is incorrect or incomplete, you may ask us to correct or update the information. You have the right to request an amendment for as long as we keep the health information. To request an amendment, you must make your request, in writing, the facility's Health Information Management Release of Information Unit and provide a reason why you are asking for an amendment. For your convenience, you may use the "*Request to Amend Protected Health Information"* form, which may be obtained from the DHS website: www.dhs.lacounty.gov or by contacting the health facility where you obtain your services.
We may deny your request for an amendment if it is not in writing or does not include a reason to support the request. We also may deny your request if you ask to amend health information that:

- Was not created by us;
- Is not part of the health information kept by or for the facility;
- Is not part of the health information that you would be permitted to inspect and copy; or,
- Is accurate and complete.

If we deny your request for amendment, in whole or in part, you have the right to submit a written statement as to what you believe is incorrect or incomplete. If you clearly state in writing that you want your statement to be made part of your medical record, we will attach it to your records and include it whenever we make a disclosure of your health information.

Right to Ask for a List of Disclosures – You have the right to request an "accounting of disclosures," which is a list of the people or organizations which we have given your health information. This list of disclosures will not include all health information we have given out. For

example, it will not include health information given out for your care, to pay for your care, for DHS business operations, or that you have authorized.

To request a copy of this list, your request must state a time period, but not longer than six years. You must submit your request to the facility's Health Information Management Release of Information Unit. For you convenience, you may use the *Request for an Accounting of Disclosures* form may be obtained from the DHS website: www.dhs.lacounty.gov or by contacting the health facility where you obtain your services. You may get one free list within a 12-month period. We may charge you for the costs of providing additional lists. We will tell you the cost at the time of your request so you can withdraw or modify your request before you are charged a fee.

Right to Ask for Restrictions on How We Use or Give Out Your Records – You have the right to ask us to follow special restrictions when using or providing your health information for treatment, payment, or health care operations. You also may ask for restrictions on the records we give out about your care to someone who is involved in taking care of you or paying for your health care, like a family member or friend. For example, you could ask us not to share information about a certain diagnoses or treatment with your spouse.

We will do our best to follow your request; however, when you fully pay out-of-pocket as explained below, we are required to agree to your request. If we do agree, we will comply with your request unless the health information is needed to provide you emergency treatment. To request a restriction, you must submit your request to the facility's Health Information Management Release of Information Unit. You must tell us (1) what information you want to limit; (2) whether you want to limit our use, disclosure or both; and (3) to whom you want the limits to apply, for example, disclosures to your spouse. For your convenience, you may complete and submit a Patient's Request for Restriction on the Use and Disclosure of Protected Health Information form, available from the DHS website: www.dhs.lacounty.gov or by contacting the health facility where you obtain your services. We will tell you if we cannot honor your request.

Right to Ask for Restrictions When You Fully Pay Out-of-Pocket -- If you or someone else paid out-of-pocket in full for a health care item or service (in other words you don't ask us to bill your health plan or health insurance company), you have the right to ask us not share information about that item or service with them. We must agree to your request, unless the law requires us to share your information. If you or someone else paid out-of-pocket in full for a health care item or service, and you wish to request this special restriction, you must submit your request to the facility's Health Information Management Release of Information Unit. For convenience, you may complete and submit a Patient's Request for Restriction on the Use and Disclosure of Protected Health Information form, available from the DHS website: www.dhs.lacounty.gov or by contacting the health facility where you obtain your services.

Right to Ask for Confidential Communications – You have the right to ask that we communicate with you about your appointments or other matters related to your treatment in a specific way or at a specific location. For example, you can ask that we only contact you at work or by mail. To request confidential communications, submit your written request to the facility's Health Information Management Release of Information Unit. Your request must specify how or where you would like to be contacted. If your request has to do with paying for care, you must tell us how you will pay if you do not want us to share your health information with persons, programs or organizations that may pay for your care. We will not ask you the reason for your request. We will accommodate all reasonable requests. For your convenience, you may submit a Patient's Request for Confidential Communications form, available from the DHS website: www.dhs.lacounty.gov or by contacting the health facility where you obtain your services.

Right to Get a Copy of This Notice – You have the right to receive a paper copy of this Notice at any time, even if you have already received a copy or have agreed to receive it electronically. You may obtain a paper copy of this Notice from the facility where you are receiving services or from your physician. This Notice is also available at the DHS website: www.dhs.lacounty.gov.

HOW DHS MAY USE AND DISCLOSE YOUR HEALTH INFORMATION

The following describes the different ways that we may use and disclose your health information. In most cases, we may use and share your health information for treatment, payment, or health care operations, without asking for your specific permission to do so.

Treatment – We create a record of the treatment and services you receive at our facilities and will use this information to provide you with medical treatment or services. We may give this information to doctors, nurses, technicians, medical students, or other facility personnel who are involved in taking care of you at the facility. We may also provide this information to doctors who work at a non-DHS facility, if they are involved in your care. For example, a doctor treating you for diabetes may need to know if you have problems with your heart because some medications affect your blood pressure. We also may share your health information, including providing it to non-DHS workforce, in order to coordinate the different things you need, such as prescriptions, blood pressure checks and lab tests, and to determine a correct diagnosis.

Payment – We will use and disclose your health information in order to get paid for the treatment and services we have provided to you. For example, we may need to give your health plan information about a medication, visit, or treatment session you received at the facility so your health plan will pay us. We may also tell your health plan about a treatment you are going to receive to obtain prior approval or to determine whether your plan will cover the treatment. We may also disclose your health information to other health care providers for their payment purposes. If you pay for your services in full, out of your pocket, you can request us to not provide your health information to third-parties such as a health insurance plan.

Health Care Operations – We may use or disclose your health information for routine business reasons, such as measuring the quality of care we provide, reviewing the performance of our staff, meeting regulatory requirements, or planning for future clinical operations. We may also share your health information with other health care facilities that have a relationship with you (such as your health plan) for their health care operation activities.

Health Information Exchange (HIE) – We, along with other health care providers in the Los Angeles area, participate in one or more health information exchanges. An HIE is a community-wide information system used by participating health care providers to share health information about you for treatment purposes. Should you require treatment from a health care provider that participates in one of these exchanges who does not have your medical records or health information, that health care provider can use the system to gather your health information in order to treat you, for example he or she may be able to get laboratory or other tests that have already been performed or find out about the treatment that you have already received. We will include your health information in this system.

Business Associates – Some services may be provided by business associates such as a billing service, record storage company, or legal or accounting consultants. We may share your health information with our business associates so they can perform the job we have asked them to do. To protect your health information, we have a written contract with our business associates that requires them to safeguard your information.

Appointment Reminders – We may use and disclose your health information to contact you to remind you about an appointment you have with us.

For Your Own Information –Your health information may be used or disclosed in order to provide you with your own test results, to tell you about treatment options or alternatives, or to provide information to you about health-related benefits or services (such as eligibility for Medi-Cal or Social Security benefits) that may be of interest to you.

Hospital Directory – DHS hospitals maintain a directory that lists patients admitted to the hospital, so family and friends can call or visit you or so you can receive mail. If you do not let us know you object, we will include your name, location in the hospital, general condition (e.g., fair, stable, critical, etc.), and religious affiliation in the hospital directory. The directory information, except for religious affiliation, will be released to people who ask for you by name, unless you have asked us not to include you or to limit this information. Providing your religious affiliation is your choice. If you decide to give us this information, it may be given to a member of the clergy, such as a priest or rabbi, even if they do not ask for you by name. This information is released so your family, friends and clergy can visit you in the hospital and generally know how you are doing.

People Who Take Care of You or Help Pay for Your Care – We may disclose your health information to a friend or family member who is involved in your medical care or payment for your health care, if you agree to this disclosure or do not object when given the opportunity to do so. Let us know if you do not want us to discuss your health information with this person. However, there may be times when we will need to use our professional judgment to decide whether the disclosure is in your best interest, such as in an emergency or if you lack the decision-making ability to agree or object or if you are not present. For example, we may allow someone to pick up a prescription for you.

Disaster Relief Purposes – We may disclose your health information to an entity assisting in a disaster relief effort so that your family can be notified about your condition, status and location. We will give you the opportunity to agree or object to this disclosure, unless we decide that we need to disclose your health information in order to respond to the emergency circumstances.

Breach Notification -- We may use and disclose your health information to tell you in the event that there has been unlawful or unauthorized access to your health information. This may include instances when someone not authorized to see your health information looks at your information or your health information is accidently lost or is stolen. We will also report these occurrences to State and federal authorities, and may need to use your health information to do so. If this happens, we will provide you with a written notice via first-class mail to your last known address.

Fundraising Activities – We may use your health information to contact you in an effort to raise money for our hospitals or clinics. For example, we may send you a letter asking if you would like to make a donation. You can chose not to be contacted for our fundraising efforts. If we send you information about our fundraising efforts, we will include a simple way for you to request that we not contact you in the future for our fundraising efforts.

Marketing – We will not use or disclose your health information for marketing purposes unless we first obtain your written authorization to do so.

Sale of Your Health Information -- Unless we first obtain your written authorization, we will not disclosure your health information to anyone if to do so would constitute a sale of your health information.

Research – Your health information may be provided to a researcher if you authorize the use of your health information for research purposes. In some situations, your health information may be released without your authorization to researchers preparing a research protocol or if our Institutional Review Board (the group that makes sure human subjects are protected during research) determines that an authorization is not required. We may also provide limited health data (not containing your name, address, or other direct identifiers) for research, public health, or

health care operations, if the person or organization that receives the information agrees to protect this information and not use it to identify you.

Disclosure Required By Law – We will provide information about you, including health information, when required to do so by federal, state, or local law, for example, the law requires us to report certain types of injuries.

To Prevent a Serious Threat to Health and Safety – Your health information may be released when necessary to prevent a serious threat to your health and safety or the health and safety of the public or another person. Your information would only be given out to someone able to help prevent the threat.

Workers' Compensation – If you were injured or became ill as a result of your employment your health information may be released for workers' compensation or similar programs that provide benefits for work-related injuries or illness.

Public Health Purposes – We may disclose health information about you for public health activities, such as preventing or controlling contagious diseases, like measles or tuberculosis; reporting births or deaths; preventing injury or disability; or reporting the abuse or neglect of children, elders and dependent adults.

Organ and Tissue Donation – If you are an organ donor, we may release health information about you to organizations that handle organ procurement or organ, eye or tissue transplantation, or to an organ donation bank to support this process.

Military Personnel and Veterans – If you are a member of the armed forces, we may release your records as required by military authorities.

Health Oversight Activities – We may provide your health information to federal, state, or local agencies for oversight activities specifically authorized by law, such as to license and inspect health care facilities.

Lawsuits and Disputes – We may provide your health information in response to a court or administrative order. We may also disclose your health information in response to a subpoena or other lawful process issued by someone involved in a legal dispute, but only if efforts have been made to inform you or to obtain an order protecting your information.

Law Enforcement - We may disclose you health information to law enforcement agencies:

- If the police bring you to the hospital and document that exigent circumstances exist to test your blood for alcohol or substance abuse

- If the police present a valid search warrant
- If the police present a valid court order
- To report abuse, neglect, or assaults as required or permitted by law
- To report certain threats to third parties or crimes committed on the premises
- To identify or locate a suspect, fugitive, material witness or missing person, if required or permitted by law
- To report your discharge, if you were involuntarily detained after a peace officer initiated a 72-hour hold for psychiatric evaluation and requested notification.

Funeral Homes, Coroners, Medical Examiners, and Information about Decedents – When required by law, your health record may be released to a coroner or medical examiner. This may be necessary, for example, to identify a deceased person or determine the cause of death. We may also release limited health information to a funeral home. We may also give health information to family members or friends of a deceased person if they were involved in the person's care or paid for that care prior to the death and the health information is relevant. However, we won't do this if the health information is not relevant to their involvement or if it is known to us that the deceased person would not have wanted us to share such information.

Specialized Government Functions – We may disclose your health information to authorized federal officials for intelligence, counterintelligence, or other national security activities authorized by law, as well as if required to protect the President, leaders of other countries, or certain other individuals.

Inmates – If you are an inmate or in the custody of law enforcement, we may release your health information to the correctional institution where you are confined or to the law enforcement official having custody. This release would be necessary to allow them to provide you with health care or to protect the health and safety of you, other inmates, or correctional staff.

Disclosures at Your Request – We may disclose your health information to a third party with your authorization. We will require that your authorization be in writing, that the authorization meet all legal requirements, and that we verify your identity.

Complaints and Investigations – The United States of Department of Health and Human Services may review our records, which may include your health information, to investigate or review our compliance with laws protecting the privacy of your health information.

Other Uses of Your Medical Information – Other uses and disclosures of your health information that are not covered by this Notice or the laws that apply to us will be made only if you authorize us to do so or if required by law. For example, we cannot use or disclose your for health information for marketing purposes, or sell your health information without your written authorization. Your authorization will remain in place until you tell us, in writing, that you are

withdrawing it. If you withdraw your authorization, we will no longer use or disclose your health information for the reasons covered by the authorization. However, we will not be able to take back any disclosures that were made when the authorization was in effect, and we are required to keep records of the care we provided to you.

CHANGES TO THIS NOTICE

We have the right to change our privacy practices in this Notice at any time. Any changes will apply to health information we already have about you as well as any health information we receive in the future. If we make major changes in the Notice, we will post the new notice, with the next effective date, in our facilities and post a copy on our website at www.dhs.lacounty.gov.

COMPLAINTS

If you think your privacy rights have been violated, you may file a complaint with Administration at the health facility where you obtain your services or any of the offices listed below.

Los Angeles County Department of Health Services
Audit and Compliance Division
313 N. Figueroa Street, Room 801
Los Angeles, CA 90012
(800) 711-5366

Los Angeles County Auditor Controller
Chief HIPAA Privacy Officer
500 West Temple Street, Suite 525
Los Angeles, CA 90012
(213) 974-2164
Email: hipaa@auditor.lacounty.gov

Region IX, Office of Civil Rights
US Department of Health and Human Services
90 7th Street, Suite 4-100
San Francisco, CA 94103
(415) 437-8310
(415) 437-8329 (Fax)
(415) 437-8311 (TDD)

DEFINITIONS:

Protected Health Information (PHI) means individually identifiable information relating to past, present or future physical or mental health or condition of an individual, provision of health care to an individual, or the past, present, or future payment for health care provided to an individual.

Workforce or *Workforce Member* includes employees, contract staff, affiliates, volunteers, trainees, students, and other persons whose conduct, in the performance of work for DHS, is under its direct control, whether or not they receive compensation from the County.

REFERENCES:

45 Code of Federal Regulations §§ 160.103, 164.530
Los Angeles County Civil Service Rules
DHS Discipline Manual and Guidelines
DHS Policy No. 747, "Disciplinary Action"

Health Services
LOS ANGELES COUNTY

POLICIES AND PROCEDURES

SUBJECT: SAFEGUARDS FOR PROTECTED HEALTH INFORMATION (PHI)

POLICY NO: 361.23

PURPOSE:

To establish safeguards to protect the security of Protected Health Information and other confidential information from unauthorized viewing, acquisition, access, use or disclosure.

POLICY:

DHS will implement appropriate administrative, technical, and physical safeguards that will reasonably safeguard protected health and confidential information from intentional or unintentional acquisition, viewing, access, use or disclosure that is in violation of DHS' Privacy Policies.

DHS' workforce must reasonably safeguard PHI to limit incidental access, use or disclosure made pursuant to an otherwise permitted or required use or disclosure.

DEFINITIONS:

Desktop Workstation, includes a stand-alone, generally stationary, personal computing device possibly connected to a network server or other computer.

Particularly Sensitive Health Information means protected health information that is generally considered highly confidential including, but not limited to, mental health, drug and alcohol abuse, and communicable disease information.

Portable Computing Devices, includes, but is not limited to, the following:

- Portable computers, including, but not limited to, laptops and tablet computers
- Portable devices, including, but not limited to, personal digital assistants (PDAs), digital cameras, smartphones, cellular telephones, and pagers
- Portable storage media, including, but not limited to, diskettes, tapes, DVDs, CDs, USB flash drives, memory cards, and external hard disk drives
- Mobile computers that can connect by cable, telephone wire, wireless transmission, or via any Internet connection to County Information Technology resources

Protected Health Information (PHI) means individually identifiable information relating to past, present or future physical or mental health or condition of an individual, provision of

health care to an individual, or the past, present, or future payment for health care provided to an individual.

Workforce or ***Workforce Member*** means employees, contract staff, affiliates, volunteers, trainees, students, and other persons whose conduct, in the performance of work for DHS, is under its direct control, whether or not they receive compensation from the County.

PROCEDURES:

The procedures below set forth minimum administrative, physical and technical safeguards regarding the protection of PHI.

I. Administrative Safeguards

A. Oral Communications. DHS' workforce must exercise due diligence to avoid unnecessary disclosures of PHI through oral communications. Enclosed offices and/or interview rooms are preferred locations for verbal exchange of PHI. Conversations involving PHI in public areas should be avoided, unless necessary to further treatment, payment, teaching, research or operational purposes. A lowered voice should be used and attention should be paid to unauthorized listeners in order to avoid unintentional disclosure of PHI. Dictation and telephone conversations should be conducted away from public areas if possible. Speakerphones should only be used in private areas and attention must be paid to the sound level.

B. Telephone Communications. Each DHS facility shall develop and implement protocols consistent with DHS guidelines to protect the confidentiality and privacy of patient information when communicating via telephone. Whenever it is necessary for DHS workforce members to discuss PHI via telephone with a patient or patient's family members or friends, other DHS workforce members, business associates, or other health care providers, workforce members must follow facility guidelines for protecting such information. Release of information over the phone may only be done if the person doing so is absolutely sure of the identity of the person he or she is speaking with and that person has a right to receive the information.

DHS workforce members will honor any agreements made with the patient or patient's personal representative regarding alternate forms of communications or restrictions on the use or disclosure of the patient's PHI. Telephone communications involving PHI should be conducted in a private area whenever

possible and in a low voice to ensure information is not overheard by unauthorized persons.

When receiving calls, DHS workforce members shall not discuss PHI with the caller until the following can be confirmed:

1. Identity of the caller (e.g., a "call back" to validate the number called, or definite voice recognition)

2. Verification that the caller has a need to know and the use and disclosure of PHI is permissible.

If confirmation cannot be made, DHS workforce members shall not confirm or deny that the patient has in the past or is currently receiving services from DHS.

C. Internet Communications. If a patient requests receipt of their PHI through the Internet, the workforce members must ensure the information is encrypted. If the information cannot be encrypted, the information must be sent through an alternate secure means of communication.

D. Telephone Messages. When making calls, DHS workforce members shall not discuss PHI until the identity of the person on the phone line has been confirmed. In the event an answering machine or voice mail system picks up the call, staff should leave a message requesting that the person they need to speak to return the call.
   - The message shall include ONLY the name and telephone number of the person that should receive the return call (e.g., "This message is for Mary Jones. Please contact Mary Smith at 555-1313).
   - Messages left on an automatic answering machine or voice mail system shall not contain PHI (e.g., diagnosis, test results, etc.).
   - Telephone messages and appointment reminders may be left on answering machines and voice mail systems, unless the patient has requested an alternate means of communication pursuant to DHS Policy No. 361.6, "Right to Request Confidential Communications of Protected Health Information (PHI)." However, each provider and/or clinic should limit the amount of PHI that is disclosed in a telephone message.
   - The content of appointment reminders should not reveal particularly sensitive health information, directly or indirectly, such as the specific name of the unit/department of the hospital.

- Telephone messages regarding test results or containing information that links a patient's name to a particular medical condition should be avoided.

E. Faxes. The following procedures must be followed when faxing PHI:

1. Only the PHI necessary to meet the requester's needs should be faxed.

2. Particularly sensitive health information should not be transmitted by fax, except in emergency situations or if required by a government agency. If particularly sensitive health information must be faxed, the recipient should be immediately notified prior to the transmission and the sender should immediately confirm the transmission was completed, if possible.

3. Workforce members should only fax PHI authorized as part of their work duties.

4. Unless otherwise permitted or required by law, a properly completed and signed authorization must be obtained prior to releasing PHI to third parties for purposes other than treatment, payment or health care operations as provided in DHS Policy 361.4, "Use and Disclosure of Protected Health Information Requiring Authorization," unless otherwise permitted or required by law. In certain instances an authorization may be needed to release information to a third party for payment, such as self-paid services, or insurance purposes.

5. PHI may be faxed to an individual if the individual requests access to their own PHI in accordance with DHS Policy 361.15, "Access of Individuals to Protected Health Information (PHI)/Designated Record Set."

6. All faxes containing PHI must be accompanied by a cover sheet that includes a confidentiality statement. Use DHS' PHI Fax Form or the form used by the facility.

7. Reasonable efforts should be made to ensure fax transmissions are sent to the correct destination. Frequently used numbers should be preprogrammed into fax machines or computers to avoid misdialing errors. Preprogrammed numbers should be verified on a routine basis. The numbers of new recipients should be verified prior to transmission.

8. Fax machines must be located in secure areas not readily accessible to visitors and patients. Incoming faxes containing PHI should not be left sitting on or near the machine.

9. Fax confirmation sheets should be reviewed to ensure the intended destination matches the number on the confirmation. The confirmation sheet should be attached to the document that was faxed. Verify receipt of the fax by contacting the intended recipient and noting such on the approved fax sheet.

10. Misdirected faxes containing PHI should be investigated and reported to the supervisor and the facility privacy coordinator. The sender should make an attempt to call the recipient to retrieve the misdirected fax, if possible. Do not read through faxes received in error: Contact the sender and advise that their fax was received in error and properly destroy the information.

F. Mail.

1. Interoffice Mail: Use a sealed envelope (not one with holes in it) and properly address the envelope with the name of the recipient as well as the location and room number. Tape the opening and stamp "confidential" over the seal.

2. Outside Mail: Use an appropriate sealed envelope for U.S. Mail. Ensure the return address does not contain the name of the department or unit within the hospital to ensure added privacy.

G. Internet/Social Networking.

Internet/social networking sites must not be used to discuss patients or patient information. Workforce members must remember that although internet/social networking sites (e.g., Twitter, Facebook, YouTube, discussion forums, text messaging, web mail, etc.) can be accessed on their own time from their own computing devices, they should remember that due to the nature of the work and the type of business they work in, just small bits of information, put together, can reveal identifying information about patients and cause them to violate privacy laws.

1. Workforce members must not disclose any confidential or proprietary information of or about the County, DHS or any of our affiliates on social networking sites.

2. Workforce members must not hold themselves out as representatives of the County or DHS or act on behalf of the County or DHS on social networking sites, unless specifically authorized in writing.

3. Workforce members, including former workforce members, may be held liable for damages and potential criminal prosecution for breaching PHI used or exposed to while working for DHS.

4. Workforce members must not engage in internet/social networking activities on their personal computing device during County work hours.

H. Photographing and Recording Patients. Photographic or audio recordings of a patient may be taken for purposes of treatment, professional education, peer review, publication, research, law enforcement, public relations, marketing and news media only upon obtaining prior written patient consent and photographs must be filed in the patient's medical record. Disclosure of photographic or audio recordings constitutes the release of medical information and therefore requires prior authorization for use or disclosure of patient health information

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

2. Authorization must contain the specific reason and use. Any other or additional use or disclosure requires a new authorization.

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

4. A workforce member's use of personal photography or recording equipment (including cellular telephones and smartphones) is prohibited.

5. Photography of medical records or any other document that contains PHI is strictly prohibited.

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

I. Destruction Standards. PHI must be discarded in a manner that protects the confidentiality of such information. Shred hardcopy documents or place them in the locked shredder bin instead of throwing them in the trash. Contact your IT/Help

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

1. PHI awaiting disposal or destruction must be stored in secure containers, storage rooms, or centralized shredder bins that are appropriately labeled and properly disposed of on a regular basis. Reasonable steps must be taken to minimize access to those documents.

2. Storage rooms containing confidential information awaiting disposal must be locked after business hours or when authorized staff are not present.

3. Centralized bins or containers used for disposal of confidential information must be sealed, clearly labeled "confidential," "PHI," or some other suitable term and placed in a secure location. Reasonable steps must be taken to minimize access to PHI.

4. Documents containing PHI must not be recycled or reused for scratch paper.

5. Portable media awaiting destruction/sanitization must be kept in a secure locked area.

II. Physical Safeguards

A. Paper Records. Paper records and medical charts must be stored or filed in such a way as to avoid access by unauthorized persons. Some type of physical barrier should be used to protect paper records from unauthorized access.

1. Paper records and medical charts on desks, counters or nurses stations must be placed face down or concealed to avoid viewing or access by unauthorized persons.

2. Paper records should be secured when the office is unattended by persons authorized to have access to paper records.

3. Original paper records shall not be removed from the premises unless permitted by law and they are secured in a manner to protect the PHI and are not to be left unattended.

4. Do not store paper records in an area where they can be thrown away or mistaken for trash.

III. Physical Access

A. Persons authorized to enter areas where PHI is stored or viewed must wear an identifiable DHS badge or be escorted by an authorized DHS workforce member.

B. Persons attempting to enter an area where PHI is processed must have prior authorization by DHS management.

C. Workforce members must not allow others to use or share their badges or keycards and must verify access authorization for unknown people entering an area where PHI is stored or processed.

IV. Visitors and Patients

Visitors, vendors, and patients must be appropriately monitored when on DHS' premises where PHI is located to ensure they do not access PHI. This means that persons who are not authorized DHS' workforce members should not be in areas in which patients are being seen or treated or where PHI is stored.

V. Desktop Workstations

PHI on computer devices must be protected from unauthorized viewing and unauthorized access. Suggested means for ensuring this protection include:

A. Using polarized screens or other computer screen overlay devices that shield information on the screen;

B. Placing computers out of the visual range of persons other than the authorized users;

C. Clearing information from the screen when not actually being used;

D. Using password protected screen savers when computer workstations are not in use.

E. Locating computers in areas that prohibit/restrict access by unauthorized individuals (e.g. not within reach of persons at counter, etc.).

VI. Remote Access or Working Offsite/Outside the Secure Work Environment

DHS employees are discouraged from removing PHI from DHS, however, it is recognized that there are some situations where work outside of the secured environment is necessary. When it is necessary for DHS staff to take patient information home or to another work environment, the following guidelines in accordance with DHS Policy 935.11, "Workstation and Mobile Device Use & Security Policy" should be followed:

A. The remote work area must provide adequate privacy and security.

B. Confidential information should be secured in locked rooms or a locked storage container when not in use.

C. Home computers must comply with DHS standards including County approved anti-virus software and must adhere to County hardware/software protection standards and procedures.

D. While on train, bus, airplane or other form of mass transit ensure use of privacy screen as well as all other requirements under section V – Desktop Workstations. Paper documents must be kept out of sight or range of view by other passengers.

E. Confidential data may not be saved on removable devices (e.g. floppy drive, CD-ROM, external drive, USB/Thumb drive) unless it is approved and appropriate safeguards are in place (e.g., encryption).

F. Data/information must not be accessible by unauthorized persons/family members. All completed work, if not remotely accessed, must be saved to the original, encrypted external device AND removed completely from the home computer.

G External devices, portable computing devices, must be encrypted and maintained in a secure location/protected from theft or loss.

VII. Technical Safeguards

Access to PHI is based on the role and job responsibilities of the workforce member. Workforce members will be assigned access to DHS' networks and systems based on their need to know and the minimum amount of information needed to fulfill their job responsibilities. Minimum necessary also applies to their access to the system. A workforce member with access to a system for completion of certain assignments is not authorized to view, use or access other information in the system not related to their job responsibilities.

A. Technical safeguards regarding the protection of PHI maintained in electronic form may include:

1. Log off any electronic system containing PHI when leaving the computer, even for a few minutes, or after obtaining necessary data.

2. Require computing devices to have a password-protected screen saver or other time-out feature.

3. All portable computing devices such as laptops, USB/thumb drives, and other electronic devices containing PHI must be encrypted.

4. Workforce members should be familiar with their facility downtime procedures.

B. Passwords

1. Workforce members are responsible for safeguarding their passwords for access to the County information technology resources.

2. Workforce members are responsible for all transactions made using their passwords.

3. Workforce members may not provide their password or use their password to provide access to another workforce member; or access the County information technology resource with another workforce member's password or account.

   Some systems have a universal access password with a secondary password neither of which shall be shared with workforce members who are not authorized to utilize the system.

4. Passwords must be changed on a regular basis to ensure security. Strong passwords include at least eight characters, such as a combination of letters, numbers and/or special characters.

5. Ensure all areas used to store PHI are properly secured and that only authorized personnel have access to those locations.

VIII. Use of Electronic Systems

DHS shall implement a combination of administrative, physical and technical safeguards to protect PHI in electronic communications networks, including (1) privacy and security awareness training of DHS Users concerning the transmission of PHI over electronic communications networks; (2) periodic review of this policy and procedure with DHS Users to confirm compliance; (3) repeated security reminders; (4) use of password-protected screen savers and exercise of due diligence to ensure that electronic systems used for transmission and/or storage of PHI is protected from viewing by unauthorized persons; and (5) other applicable safeguards outlined in this Policy.

A. Portable Computing Devices

1. All portable computing devices that access and/or store PHI or confidential information must comply with all applicable DHS and County IT resources policies, standards, and procedures.

2. Generally, DHS prohibits the download or storage of PHI and/or confidential information on portable computing devices. However, DHS Users who, in the course of County business, must download or store PHI and/or confidential information on portable computing devices are required to adhere to DHS policies and procedures for storage and use of PHI and/or confidential information on portable computing devices.

3. If PHI and/or confidential information is downloaded or stored on a portable computing device, information must be protected from unauthorized access and, without exception, the information must be encrypted.

4. A DHS User who intends to use their County-owned or personally owned portable computing device to access and/or store PHI and/or confidential

information is required to obtain prior written authorization from the DHS Information Technology.

B. E-Mail

1. Non-County e-mail such as G-Mail, Yahoo Mail, etc. must not be used for sending DHS-related PHI. Use of e-mail between a DHS User and a patient is permitted provided that the e-mail is encrypted and sent through the County's e-mail system.

2. Replying to e-mail with patient, confidential, and/or sensitive information: DHS users must follow the same procedures when replying to e-mail with patient, confidential, and/or sensitive information in the same manner as if it were originally created by the DHS User.

3. Audits of outbound e-mail communications may be periodically performed to ensure that use of e-mail to transmit PHI is in accordance with Departmental policies. Refer to DHS Policy 935.20, Acceptable Use Policy for County Information Technology Resources."

C. Online Web-based Document Sharing Services

Storing and/or sharing of PHI and other confidential information using non-County approved online web-based document sharing services (e.g., Google Docs, Microsoft Office Live, Open-Office, Dropbox, etc.) is strictly prohibited.

IX. Disciplinary Action

Unauthorized viewing, acquisition, access, use, or disclosure of confidential and/or protected health information (including but not limited to medical records) will result in disciplinary action, up to and including discharge, as well as possible civil/criminal penalties, fines and disciplinary action against the individual's professional license, permit, registration, or certificate from the issuing board or agency.

X. Document Retention

This policy will be retained for a period of at least 6 years from the date of its creation or the date when it was last in effect, whichever is later.

REFERENCES:

45 Code of Federal Regulations, Part 164, Section 164.530(c)(1)
DHS Policy Numbers:

361.6	Right to Request Confidential Communications of Protected Health Information
361.15	Access of Individuals to Protected Health Information (PHI)/Designated Record Set
361.26	Mitigation
935.043	Blackberry Handheld Devices for Remote GroupWise Access Policy
935.11	Workstation & Mobile Device Use and Security Policy
935.20	Acceptable Use Policy for County Information Technology Resources

DHS Discipline Manual and Guidelines

Health Services
LOS ANGELES COUNTY

POLICIES AND PROCEDURES

SUBJECT: ACCEPTABLE USE OF COUNTY INFORMATION TECHNOLOGY RESOURCES

POLICY NO: 935.20

PURPOSE:

To ensure the entire Department of Health Services (DHS) workforce follow acceptable use of County information technology resources within the department.

POLICY:

Each DHS workforce member is required to adhere to and management is expected to strictly enforce all policies and procedures with respect to the proper use of County information technology resources in accordance with DHS Policy No. 361.1, DHS Privacy and Security Compliance Program, the County Fiscal Manual, and other County and DHS information technology use policies and procedures.

All workforce members are required to sign acknowledgment of the receipt and review of the County and DHS' Acceptable Use policy (as noted below). DHS Human Resources must ensure that each new hire or transferred County workforce member receives and signs the following documents during in-processing

1) *County of Los Angeles Agreement of Acceptable Use and Confidentiality of County's Information Technology Assets, Computers, Networks, Systems and Data (County Acceptable Use Agreement)* and,
2) Acknowledgment of this policy

Managers/supervisors must review both documents and have them signed and completed by each County workforce member during the annual performance evaluation process.

Each Non-County workforce member shall receive and acknowledge the "DHS Comprehensive Policy Statement" in accordance with the non-County workforce member in-processing procedures. The "DHS Comprehensive Policy Statement" must also be provided to and acknowledged by the non-County workforce member in conjunction with their annual performance review process.

APPROVED BY: [signature]
REVIEW DATES: 8/14/12

EFFECTIVE DATE: August 15, 2012
SUPERSEDES: September 1, 2009

DHS System Managers/Owners will ensure that all workforce members with access to County information technology resources have signed the agreement and acknowledgment prior to providing access.

I. RESPONSIBILITY

Access to County information technology resources and accounts is a privilege granted to workforce members based on their job duties and may be modified or revoked at any time. Each workforce member is responsible for the protection of DHS' County information technology resources. Workforce members must protect all Information contained in the technology resources as required by local, state and federal laws and regulations. Each workforce member must sign and abide by the County Acceptable Use Agreement and the provisions of this policy.

County workforce members will be required to sign the County Acceptable Use Agreement and the acknowledgment at the time of new hire or transfer into DHS and annually as part of the performance evaluation process. Non-County workforce members will be required to acknowledge the County Acceptable Use Agreement and this policy by signing the "DHS Comprehensive Policy Statement" during the in-processing procedure and in conjunction with their annual performance review.

The completed acknowledgment forms must be filed in the workforce member's personnel folder. Acknowledgments from the "DHS Comprehensive Policy Statement" will be filed in the non-County workforce member's Human Resources file.

Violation of the County Acceptable Use Agreement or this policy may result in disciplinary action, up to and including, discharge and possible civil and/or criminal liability.

Non-County workforce members found to be in violation of the County Acceptable Use Agreement or this policy may be released from assignment and recorded as a "do not send" in the DHS "Do Not Send" Database.

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

II. WORKFORCE MEMBER PRIVACY

Workforce members have no expectation of privacy with respect to their use of the County information system assets, because at any time DHS may log, review, or monitor any data created, stored, accessed, sent, or received. DHS has, and will exercise, the right to monitor any information stored on a workstation, server or other storage device; monitor any data or information transmitted through the DHS network; and/or monitor sites visited on the DHS Intranet, Internet, chat groups, newsgroups, material downloaded or uploaded from the Internet, and e-mail sent and received by workforce members. Activities, communications, or computer usage not related to County business are likely to be monitored. DHS may use manual or automated means to monitor use of its County information technology resources.

A supervisor/manager may request to review the system activities of a subordinate if misuse of DHS system resources is suspected. If evidence of misuse of DHS system resources is identified, the supervisor/manager must contact the DHS Audit & Compliance Division to determine appropriate actions. The DHS Audit & Compliance Division may also be required to contact the Auditor-Controller's Office of County Investigations.

Violations involving non-County workforce members shall be referred to the Facility Liaison/Contract Monitor for appropriate action.

Use of passwords to gain access to County information technology resources or to encode particular files or messages does not imply any expectation of privacy in the material created or received. The requirement for use of passwords is based on DHS' obligation to properly administer information technology resources to ensure the confidentiality, integrity and availability of Information. Workforce members are required to authenticate with a unique Employee/Workforce member ID so that all access may be auditable.

III. PROHIBITED ACTIVITIES

A. Prohibited Uses: Workforce members are prohibited from using County information technology resources for any of the following activities:

1. Engaging in unlawful or malicious activities.

2. Sending, receiving or accessing pornographic materials.
3. Engaging in abusive, threatening, profane, racist, sexist or otherwise objectionable language.
4. Misrepresenting oneself or the County.
5. Misrepresenting a personal opinion as an official County position.
6. Defeating or attempting to defeat security restrictions on County systems or applications.
7. Engaging in personal or commercial activities for profit.
8. Sending any non-work related messages.
9. Broadcasting unsolicited, non-work related messages (spamming).
10. Intentionally disseminating any destructive program (e.g., viruses).
11. Playing games or accessing non-business related applications, or social networking sites.
12. Creating unnecessary or unauthorized network traffic that interferes with the efficient use of County information technology resources (e.g., spending excessive amounts of time on the Internet, engaging in online chat groups, listening to online radio stations, online shopping).
13. Attempting to view and/or use another person's accounts, computer files, program, or data without authorization.
14. Using County information technology resources to gain unauthorized access to DHS or other systems.
15. Using unauthorized wired or wireless connections to DHS networks;
16. Copying, downloading, storing, sharing, installing or distributing movies, music, and other materials currently protected by copyright, except as clearly permitted by licensing agreements or fair use laws.
17. Using County information technology resources to commit acts that violate state, federal and international laws, including but not limited to laws governing intellectual property.
18. Participating in activities that may reasonably be construed as a violation of National/Homeland security.
19. Posting scams such as pyramid schemes and make-money-quick schemes.
20. Posting or transmitting private, proprietary, or confidential information, including patient information, to unauthorized persons, or without authorization.
21. Downloading confidential or patient information or data onto a mobile storage device without authorization from the Facility CIO/designee.

22. Using Online Web-based Document Sharing Services (e.g., Google Docs, Microsoft Office Live, Open-Office) to store or share DHS data.
23. Viewing, accessing, using or disclosing confidential or patient information or data if not authorized as part of the workforce member's job duties.

B. Misuse of software: Workforce members must not engage in software copyright infringements. Workforce members are prohibited from conducting the following activities without proper licensing and prior written authorization by the Facility CIO/designee:

1. Copying County-owned software onto their home computers.
2. Providing copies of County-owned software to independent contractors, clients or any other third-party person.
3. Installing software on any DHS workstation (e.g., desktops, personal computers, mobile devices, and laptop) or server, unless authorized by their supervisors and IT management.
4. Downloading software from the Internet or other online server to DHS workstations or servers.
5. Modifying, revising, transforming, recasting or adapting County-owned software.
6. Reverse-engineering, disassembling or decompiling County-owned software.

IV. PASSWORDS

Workforce members are responsible for safeguarding their passwords for access to the County information technology resources. Workforce members are responsible for all transactions made using their passwords. Workforce members may not provide their password or use their password to provide access to another Workforce member; or access the County information technology resource with another Workforce member's password or account. Some systems have a universal access password with a secondary password neither of which shall be shared with workforce members who are not authorized to utilize the system. Workforce members should be aware that leaving a computer unattended for a brief time, even 30 seconds, may give an unauthorized user enough time to access the system using the previous user's access.

V. SECURITY

A. County information technology resources

Workforce members are responsible for ensuring that the use of outside computers and networks, such as the Internet, do not compromise the security of County information technology resources. This responsibility includes taking reasonable precautions to prevent intruders from accessing County information technology resources.

B. Malicious software

Malicious software can cause substantial damage or inconvenience to County information technology resources. Workforce members are responsible for taking reasonable precautions to ensure that they do not introduce malicious software into County information technology resources. Workforce members must not bypass or disable County malicious software protections. Workforce members must only use or distribute storage media or e-mail (including attachments) known to the workforce member to be free from malicious software.

Any workforce member who telecommutes or is granted remote access must utilize equipment that contains current County-approved anti-virus software and must adhere to County hardware/software protection standards and procedures that are defined by the County and the authorizing Department.

DHS restricts access to the Internet or any other network via modem, cellular wireless, or other telecommunication services. No workforce member may employ any external inbound or outbound connections to DHS network resources unless explicitly authorized by the Departmental Information Security Officer (DISO) or designee.

Each workforce member is responsible for notifying the Department's Help Desk or the Department Security Contact as soon as a device is suspected of being compromised by a virus.

VI. E-MAIL

Access to County e-mail services is a privilege that may be wholly or partially restricted without prior notice and without consent of the workforce member. E-mail messages are the property of the County and subject to review by authorized County personnel.

E-mail messages are legal documents. Statements must not be made on e-mail that would not be appropriate in a formal memo. Workforce members must endeavor to make each electronic communication truthful and accurate. Workforce members are to delete e-mail messages routinely in accordance with both the DHS and County E-mail policies.

Protected Health Information (PHI) and other confidential and/or sensitive information can only be sent or received if it is encrypted or safeguarded in accordance with DHS Policy No. 361.23, Safeguards for Protected Health Information (PHI).

Access to Internet-based e-mail sites (e.g., Yahoo Mail, Google Mail, Hotmail, etc.) is not permitted. Exceptions to this policy must be based upon requirements to perform job-related activities and be approved by DHS management.

Default E-Mail Retention Period

DHS e-mail systems will be configured to **automatically delete** messages greater than **three years** on active e-mail servers. This auto-delete policy applies to messages within all folders (inbox folders, sent file folders, draft file folders, etc.) stored on active e-mail servers. DHS will have three levels of e-mail users. (Level 1 is 3 years, Level 2 is 5 years, and Level 3 is 7 years of retention time)

All DHS e-mail system users are expected to:

1. Regularly check for new messages;
2. Delete **transitory** messages as quickly as possible.

    a. Specially defined groups will have a maximum of either a five or seven year retention period.
    b. Specially defined groups may consist of members from Audit and Compliance, Risk Management, Human Resources, Finance, and facility CEO's.

c. Facility CEO's and Executive Management from defined groups will determine which individuals will be allowed a five or seven year retention period.
d. No Personal Storage Table, (PST) files will be allowed or used by DHS e-mail users.
e. E-mail is not to be used for the storage of patient/protected health information of any kind, nor is it to be used as a document storage system.

VII. USE OF THE INTERNET

Use of the Internet must be in accordance with DHS and County Internet and privacy policies.

All DHS Internet activities are monitored and audited by DHS Security Operations and Compliance Divisions.

Unauthorized non-County business Instant Messaging and Streaming Media are strictly prohibited.

Workforce members must not allow another workforce member to access the Internet using their authorized account.

DHS is not responsible for material viewed or downloaded by workforce members from the Internet. The Internet is a worldwide public network that is uncensored and contains sites that may be considered offensive. Workforce members accessing the Internet do so at their own risk and DHS shall not be liable for inadvertent exposure to any offensive materials.

Internet access is provided to the workforce member at the discretion of each DHS Facility.

VIII. INFORMATION TECHNOLOGY USER ACCOUNT MANAGEMENT

When a workforce member leaves the County service, the supervisor must inform the local service desk to have the workforce member's Information Technology (IT) user accounts deactivated immediately. All IT accounts that have been deactivated for 60 days or more will be deleted. The workforce member's supervisor will be

contacted for approval to delete the accounts. In cases where the supervisor failed to inform the local service desk, Human Resources records will be used to disable accounts that have not been active in the last 60 days. All IT accounts that have been inactive for 60 days or more will be deleted.

Each Facility's Information Technology Department shall adhere to this minimum standard/guideline.

Each Facility's Information Technology Department shall develop and implement procedures to ensure compliancy.

IX. RECORDABLE MOBILE DEVICES AND REMOVABLE MEDIA

Workforce members must manage and control all recordable mobile devices and removable media that contain PHI or other confidential information. These devices include PDA's, USB flash drives, personal cell phones, cameras, removable hard disks, CD-R, CD-RW, DVD-R, DVD-RW and floppy disks.

The use of recordable mobile devices and removable media must be pre-approved and registered for use by the Facility CIO/designee in accordance with DHS Policy No. 935.11, Workstation Use and Security : Access and Use of Mobile Devices and DHS Policy No. 935.13 Device and Media Controls: Accountability.

X. REMOTE ACCESS SERVICES

No workforce member may employ any remote inbound or outbound connections to DHS network resources unless explicitly authorized by the Departmental Information Security Officer (DISO) or designee.

Unauthorized Remote Access Services (e.g., LogMeIn, GoToMyPC) are strictly prohibited.

Any workforce member who is granted remote access to the DHS network must utilize the approved DHS Information Security method for remote access. VPN is the DHS approved remote access solution until further notice.

Dial-up, DSL, modem etc. are strictly prohibited.

At no time should any workforce member share their remote access privileges with anyone, including other workforce members or family members.

DEFINITIONS:

INFORMATION TECHNOLOGY RESOURCES/ASSETS Any equipment or interconnected system or subsystems of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; including computers; ancillary equipment; software, firmware, and similar procedures; services, including support services; and related resources.

INFORMATION TECHNOLOGY USER ACCOUNTS An authorized user account (i.e., E-mail, Internet, Network File Share, Health Information System, etc.) provided to a user, to be used solely by that user, for the purpose of accessing services as granted to that user account.

WORKFORCE MEMBER Employees, contract staff, affiliates, volunteers, trainees, students, and other persons whose conduct, in the performance of work for DHS, is under its direct control, whether or not they receive compensation from the County.

MALICIOUS SOFTWARE The collective name for a class of programs intended to disrupt or harm systems and networks. The most widely known example of malicious software is the computer virus; other examples are Trojan horses and worms.

PERSONAL STORAGE TABLE A file that stores e-mail messages, calendar events and contact information used in applications such as Microsoft Outlook.

REMOTE ACCESS SERVICE A service that supports connecting a PC from a location outside of the DHS network (e.g. home) to the DHS network or vice versa.

For a more complete definition of terms used in this policy and/or procedure, see the DHS Information Security Glossary, Attachment I to DHS Policy No. 935.00 DHS Information Technology and Security Policy.

AUTHORITY:

Board of Supervisors Policies:
- 6.101, Use of County Information Technology Resources
- 6.102, Countywide Antivirus Security Policy
- 6.104, Use of Electronic Mail (E-mail) by County Employees
- 6.105, Internet Usage Policy

CROSS REFERENCES:

DHS Policy Nos.:
- 361.1, DHS Privacy and Security Compliance Program
- 361.23, Safeguards for Protected Health Information (PHI)
- 935.00, DHS Information Technology and Security Policy
- 935.11, Workstation Use and Security
- 935.13, Device and Media Controls

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.

 Initial _____

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.**

12. 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) wrongfully 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.

 Initial _____

(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 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.

ACKNOWLEDGMENT:

I acknowledge that I have received and read the Department of Health Services' Policy No. 935.20, DHS 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 or release from assignment.

If I have any questions concerning the policy or agreement, I will discuss them with my supervisor.

Name (print):	Employee/Contractor ID No.:	Date:
Signature:	Job Title:	Department No.:
Supervisor Name (print)	Supervisor Signature:	Date:

DHS Policy No. 935.20 Rev 7/6/12

Initial _____

ACKNOWLEDGMENT OF RECEIPT

PRIVACY AND SECURITY SURVIVAL TRAINING: PROTECTING PATIENT INFORMATION HANDBOOK

My signature on this form below confirms my receipt of this handbook, the DHS Notice of Privacy Practices (NPP) and the following DHS policies:

- 361.10, "Disciplinary Actions for Failure to Comply with Privacy Policies and Procedures;
- 361.23, "Safeguards for Protected Health Information (PHI);" and
- 935.20, "Acceptable Use Policy for County Information Technology Resources"

I acknowledge that I have read and been informed about the content, requirements and expectations of me as a DHS workforce member regarding confidential information.

I understand that if I have questions, at any time, regarding the access, use and/or disclosure of confidential information, I may consult with my immediate supervisor, the facility Privacy (or Information Security) Coordinator or DHS Privacy Officer or the DHS Information Security Officer.

I also acknowledge that I will complete the following online trainings: "Compliance Awareness Training" and "Privacy and Security Survival Training: Protecting Patient Information" within 60 days of my hire or assignment.

_____	_____	_____
Workforce Member Name (Print)	Workforce Member ID/Emp#	Date

_____

Workforce Member Signature