

# **2009 Basic Privacy and Security HIPAA Training**

What Is **H** **I** **P** **A** **A** “**HIPAA**”?

## **HIPAA is a Federal Law enacted to:**

- Protect the privacy of a patient’s personal and health information
- Provide for the physical and electronic security of personal health information
- Simplify billing and other transactions with Standardized Code Sets and Transactions
- Specify new rights of patients to approve access/use of their medical information

## **Do the HIPAA laws apply to you?**

The Health Insurance Portability & Accountability Act (HIPAA) requires that UCLA train all members of its workforce about the University’s HIPAA Policies and specific procedures required by HIPAA that may affect the work you do for UCLA Medical Sciences which includes the UCLA Hospital System, Faculty Group Practice and David Geffen School of Medicine (referred herein as University).

---

## **Answer These Questions**

- 1. HIPAA is a federal law enacted to protect the privacy of a patient’s personal and health information and provide for its physical and electronic security.**
  - a. True
  - b. False
  
- 2. Who has to follow the HIPAA Law?**
  - a. Physicians
  - b. Physicians and all Other Patient Care Providers
  - c. Only supervisors and other administrators
  - d. All University workforce members

## What are the HIPAA requirements?

- To protect the **privacy and security** of an individual's Protected Health Information (PHI)
- To require the use of "**minimal necessary**"
- To extend the **rights of individuals** over the use of their PHI

\*Use includes accessing or looking up a patient record in any of the University systems or paper records which is NOT required for your job.



Health Information with identifiers =  
**Protected Health Information (PHI)**

## What Patient Information Must We Protect?

### We must protect an individual's personal and health information that...

- Is created, received, or maintained by a health care provider or health plan
- Is written, spoken, or electronic
- And, includes at least one of the 18 personal identifiers in association with health information

### Protected Health Information (PHI): 18 Identifiers defined by HIPAA

- |   |   |
|---|---|
| <input checked="" type="checkbox"/> Name                              | <input checked="" type="checkbox"/> License numbers   |
| <input checked="" type="checkbox"/> Postal address                    | <input checked="" type="checkbox"/> Medical record number   |
| <input checked="" type="checkbox"/> All elements of dates except year | <input checked="" type="checkbox"/> Health plan beneficiary #                                     |
| <input checked="" type="checkbox"/> Telephone number                  | <input checked="" type="checkbox"/> Device identifiers and their serial numbers                   |
| <input checked="" type="checkbox"/> Fax number                        | <input checked="" type="checkbox"/> Vehicle identifiers and serial number                         |
| <input checked="" type="checkbox"/> Email address                     | <input checked="" type="checkbox"/> Biometric identifiers   |
| <input checked="" type="checkbox"/> URL address                       | <input checked="" type="checkbox"/> (finger and voice prints)                                     |
| <input checked="" type="checkbox"/> IP address                        | <input checked="" type="checkbox"/> Full face photos and other comparable images                  |
| <input checked="" type="checkbox"/> Social security number            | <input checked="" type="checkbox"/> Any other unique identifying number, code, or characteristic. |
| <input checked="" type="checkbox"/> Account numbers                   |   |

---

### Answer These Questions

#### 3. What does PHI stand for?

- Physical Health Injuries
- Patient and Hospital Incidents
- Personal and Health Information
- Protected Health Information

#### 4. Under what circumstances are you free to repeat to others PHI that you hear on the job?

- Only if you know a patient won't mind
- After you no longer work at the organization
- After a patient dies
- When your job requires it

#### 5. Protected Health Information (PHI) includes:

- name, address, birth date, SS#, email address
- medical records, diagnosis, treatment, test results
- billing records, census reports, referral authorizations
- all of the above

## **In order for the University to use or disclose PHI**

- The University must give each patient a Notice of Privacy Practices which:
  - Describes how the University may use and disclose the patient's protected health information (PHI) *and*
  - Advises the patient of his/her privacy rights
- The University must attempt to obtain a patient's signature acknowledging receipt of the Notice, EXCEPT in emergency situations. If a signature is not obtained, the University must document the reason it was not.
- 45 CFR164.520(a)(b)

**But**, for purposes other than treatment, payment, operations... Unless required or permitted by law the University must obtain authorization from the patient to use, disclose or access only the minimum necessary:

- Patient Authorization - allows for University to disclose information for other purposes (§164.508)
- Minimum necessary applies to all uses and disclosures for payment and all healthcare operations (§164.502(b), §164.514(d))

---

### **Answer These Questions**

**6. Under HIPAA, patients have certain rights contained in the following documents:**

- a. Confidentiality Statement
- b. Notice of Privacy Practices
- c. Condition on Admission
- d. Authorization Form

**7. Your sister's best friend just had triple bypass surgery at the medical center. Your sister asks you to find out his prognosis. What should you do?**

- a. Ask a nurse on the floor how the patient is doing and pass the information along to your sister.
- b. Log into Essentris and PCIMS and pass the information along to your sister.
- c. Explain that it's a violation of the patient's privacy for you to ask around or look at his record.
- d. None of the above.

**8. After a patient receives the Notice of Privacy Practices, when can the University access or disclose PHI?**

- a. For treatment of a patient
- b. For payment of bills
- c. For healthcare operations
- d. All of the above.

## With All of the State and Federal Laws, what Patient Information Must Be Protected?

**All personal and health information that exists for every individual in any form:**

- Written
- Spoken
- Electronic

**This includes HIPAA protected health information and confidential information under State laws.**

**To the patient, it's all confidential information**

- Patient ***Personal*** Information
- Patient ***Financial*** Information
- Patient ***Medical*** Information
  - Written, Spoken, Electronic ***PHI***

---

### Answer These Questions

- 9. State and Federal laws, as well as University policy, require what form of PHI to be protected and remain confidential?**
- a. Written
  - b. Spoken
  - c. Electronic
  - d. All of the above

## Why me?

**I do not provide Patient Care...do I Need Training?**

**I do not use or have contact with patient health or financial information...  
do I need training?**

**And...**

**Isn't this just an IT Problem?**

---

### Who Uses PHI at UCLA?

- **Anyone** who works with or may see health, financial, or confidential information with HIPAA PHI identifiers
- **Everyone** who uses a computer or electronic device which stores and/or transmits information
- Such as:
  - Health System employees
  - Faculty Group Practice employees
  - David Geffen School of Medicine employees
  - Campus staff who work in clinical areas
  - Administrative staff with access to PHI
  - Volunteers
  - Students who work with patients
  - Research staff and investigators
  - Accounting / Payroll staff
  - Almost **Everyone** – at one time or another!

---

### Answer These Questions

**10. Because I have access to confidential patient information as part of my job, I can look up anybody's record, even if they are not my patient, as long as I keep the information to myself.**

- a. True
- b. False

## Why is protecting privacy and security important?

### When should you:

- Look at PHI?
- Use PHI?
- Share PHI?

**Answer: Only when required for treatment, payment or healthcare operations or when permitted or required by law.**

---

### Answer These Questions

#### 11. You can protect patient information by:

- a. Protecting verbal or written information
- b. Utilizing safe computing skills
- c. Reporting suspected security incidents
- d. All of the above

---

### HIPAA Scenario #1

*I work in admitting. A friend who works in the ER told me that she just saw a famous movie star get on the elevator. My friend read in the paper that the movie star has cancer and asked me to find out what floor the star is on because we know which floors are where cancer patients are treated.*

### Ask yourself these questions:

- Do you need to know which floor the movie star is on for you to do your job?
- Does your friend need to know if the movie star has cancer for her to do her job?
- Would you want strangers to have your private information?

## Answer These Questions

12. A 19-year-old UCLA student is admitted through the ER for injuries sustained in a motor vehicle accident. She is in stable condition, but awake and alert. Her father calls from Minnesota asking for information on her condition. You can:
- Tell the patient's father of her general condition and status
  - Provide no information at all to her father
  - Obtain patient consent to provide more than her general condition and status
  - Both a and c.
13. News reporter comes into the ER and tells the attending physician that there is suspicion that the accident in which the 19-year-old female was injured was caused by a sniper shooting on the freeway and he is doing a story for the nightly news. He wants the patient's name and condition for his report. You can provide him with this information.
- True
  - False

---

## HIPAA Scenario #2

*I am a file clerk. While opening lab reports, I saw my manager's pregnancy test results. Her pregnancy test was positive! That night at a holiday party, I saw her with some friends, and congratulated her on her pregnancy. Later I heard that she did not know about the test results. I was the first person to tell her! -- Did I do the right thing?*

### Ask yourself:

- Did you need to read the lab results to do your job?
- Is it your job to provide a patient with her health information—even if the individual is a friend or fellow employee?
- Is it your job to let other people know an individual's test results?
- Should a University employee look at another employee's medical information if it is NOT required for his/her job?
- How would you feel if this had happened to you?

**Do not look at, read, use or tell others about an individual's PHI unless it is part of your job.**

## Answer These Questions

**14. A physician is very busy and asks you to log into the clinical information system using his/her user-ID and password to retrieve some patient reports. What should you do?**

- a. It's a physician, so it's okay to do this.
- b. Ignore the request and hope she forgets.
- c. Decline the request and refer to the UC Information Security Policies.
- d. None of the above.

**15. A co-worker is called away for a short errand and leaves the clinic PC logged onto the confidential information system. You need to look up information using the same computer. What should you do?**

- a. Log your co-worker off and re-log in under your own User ID and password.
- b. To save time, just continue working under your co-worker's User-ID.
- c. Wait for the co-worker to return before disconnecting him/her; or take a long break until the co-worker returns.
- d. Leave your co-worker's computer logged on and find a different computer to use.

## Reminders

- ***Use only if necessary to perform job duties***
- ***Use the minimum necessary to perform you job***
- ***Follow UCLA Medical Sciences or UCLA campus policies and procedures for information confidentiality and security.***

## HIPAA Violations Can Carry Penalties—

- **Criminal Penalties**
  - \$50,000 - \$250,000 fines
  - Jail Terms up to 10 years
- **Civil Monetary Penalties**
  - \$100 - \$25,000/yr fines
  - More \$ if multiple year violations
- **Fines & Penalties – Violation of State Law**
  - Staff may be fined per violation and reported to their licensing board if applicable
- **UCLA Corrective & Disciplinary Action**
  - Up to & including loss of privileges and job loss

## How Can You Protect Patient Information: PHI / ePHI /Confidential

- Verbal Awareness
- Written Paper / Hard Copy Protections
- Safe Computing Skills
- Reporting Suspected Security Incidents

### Patients can be concerned about...

- Being asked to **state out loud** certain types of confidential or personal information
- **Overhearing conversations** about PHI by staff performing their job duties
- Being asked about their private information in a “**loud voice**” in public areas, in
  - clinics, waiting rooms, service areas
  - hallways, in elevators, on shuttles, on streets

## Protecting Privacy: Verbal Exchanges

- Patients may see normal clinical operations as violating their privacy (*incidental disclosure*)
- Ask yourself: “**What if it was my information being discussed in this place or in this manner?**”

### Incidental disclosures and HIPAA

- “**Incidental**”: a use or disclosure that cannot reasonably be prevented, is limited in nature and occurs as a by-product of an otherwise permitted use or disclosure. (§164.502(c)(1)(iii))
  - Example: discussions during teaching rounds; calling out a patient’s name in the waiting room; sign in sheets in hospital and clinics.

## Answer These Questions

**16. The entire contents of a celebrity's mobile phone (blackberry) have appeared on the Internet, including private emails, addresses and phone numbers from the phone address book. The mobile network appears to have been hacked. A physician has similar information on his/her blackberry including a photo of a patient (obtained with patient consent) to download into an educational presentation. How can this MD best protect this information?**

- a. Download the photo immediately after taking, and delete the image from the phone.
- b. Don't take photos of patients on this type of device.
- c. Only keeps information on your mobile phone that you have no problem being posted on a public site.
- d. All of the above

---

## Incidental disclosures and HIPAA

- Incidental uses and disclosures are permitted, so long as reasonable safeguards are used to protect PHI and minimum necessary standards are applied.
- Commonly misunderstood by patients!

## Information can be lost...

---

## Answer These Questions

Please ✓ check the best answer that applies.

**17. Accessing any site on the internet can be tracked back to your name and location.**

- a. True
- b. False

## **We need to protect the entire lifecycle of PHI**

- Intake/creation
- Storage
- Destruction
- For any format

**Shredding bins work best when papers are put inside the bins. If it's outside the bin, it becomes:**

- × Daily gossip
- × Daily trash
- × Public

## **Electronic PHI can also be lost or stolen**

- Lost/stolen laptops, PDAs, cell phones
- Lost/stolen zip disks, CDs, floppies, flash drives
- Unprotected systems were hacked
- Email sent to the wrong address or wrong person (faxes have same issues)
- User not logged off of system

**Be aware that ePHI is everywhere**

---

### **Answer These Questions**

Please ✓ check the best answer that applies.

**18. From Florida (Feb 2005): An email attachment with an unencrypted list of HIV patients was sent in error to 10 individuals outside the organization (names, MRN's, SSN's and diagnoses). What actions should be taken?**

- a. The user should notify Computer Services immediately.
- b. Computer services staff should act on the notice immediately.
- c. Computer Security Official should notify the 10 recipients and requested that the file be deleted. Incident and corrective actions should be documented and reported within 5 days to the CA Department of Public Health and the affected patients and legal representatives.
- d. All of the above.

**19. I do not work with patients or have access to medical records, however, I see patients pass by my desk in the clinic. Can't I talk about the patients with my coworkers, family and friends even if it has nothing to do with my job?**

- a. You may only talk about the patients with your coworkers only
- b. You may only talk about the patients with you family and friends
- c. You may discuss the patients with coworkers and family & friends
- d. You may NOT discuss any PHI with anyone unless required for your job.

## “Good Computing Practices” 10 Safeguards for Users


- Passwords
- Lock Your Screen
- Workstation Security
- Portable Device
- Data Management
- Anti Virus
- Computer Security
- Email
- Safe Internet Use
- Reporting Security Incidents / Breach

## Good Computing Practices #1 Passwords

Use cryptic passwords that can't be easily guessed and protect your passwords - don't write them down and don't share them!

## Good Computing Practices #2 Lock Your Screen

### **For a PC ~**

- <ctrl> <alt> <delete> <enter>
- or
-  <L>

### **For a Mac ~**

- Configure screensaver with your password      Create a shortcut to activate screensaver
- Use a password to start up or wake-up your computer.

## Good Computing Practices #3 Workstation Security

### ❖ **Physically secure your area and data when unattended**

## Good Computing Practices #4 Portable Device Security

### ❖ **Don't keep confidential data on portable devices**

### ❖ **Back-up your data**

- ✓ Make backups a regular task, ideally at least once a day.
- ✓ Backup data to your department's secure server or store on removable media such as CD-RW or a USB memory stick.
- ✓ Store backup media safely and separately from the equipment. Remember, your data is valuable!

### **Data Back-ups, Ask yourself...**

- How effective would you be if your email, word processing documents, excel spreadsheets and contact database were wiped out?
- How many hours would it take to rebuild that information from scratch?

## Good Computing Practices #5 Data Management

### **Managing Confidential Data**

- Know where this data is stored.
- Destroy confidential data which is no longer needed ~
  - **Shred** or otherwise destroy confidential data before throwing it away
  - **Erase/degauss** information before disposing of or re-using drives
- Protect confidential data that you keep ~
  - **Back-up** your data to a departmental server

## Good Computing Practices #6 Anti Virus





**Make sure your computer has anti-virus and all necessary security patches.**

## Good Computing Practices #7 Computer Security




**Do Not install unknown or unsolicited programs on your computer.**

## Good Computing Practices #8 Email

### Practice safe emailing

-  Don't open, forward, or reply to suspicious emails
-  Don't open suspicious email attachments or click on unknown website addresses
-  Delete spam
-  Before emailing patients, confirm a valid email consent is in the medical record

## Good Computing Practices #9 Safe Internet Use

-  Accessing patient information electronically can be tracked back to your User ID and computer and defines the documents and time spent accessing the records.
-  Accessing sites with questionable content often results in spam or release of viruses.
-  And it bears repeating...Don't download unknown or unsolicited programs!

## Good Computing Practices #10 Reporting Security Incidents/ Breach

**How to Report Security Incidents/ Breach?** Report lost or stolen laptops, Blackberries, PDAs, cell phones, flash drives, etc...

Loss or theft of any computing device **MUST** be reported immediately to the UCLA Police Department. **Dial 1-310-825-1491**

√ In addition, immediately report anything unusual, suspected security incidents, or breaches to your Computing Support Coordinator and supervisor. University areas should call the MCCS Help Desk, (310) 794-4357.

√ This also applies for loss/theft of PHI in hardcopy format (paper, films etc).

√ You can also contact the Medical Sciences Information Security Officer

Ann S. Chang, CISSP  
achang@mednet.ucla.edu  
(310) 825-7003

---

### Answer These Questions

**20. Which workstation security safeguards are YOU responsible for using and/or protecting?**

- a. User ID
- b. Password
- c. Logging out of programs that access PHI when not using them.
- d. All of the above

# RESOURCES

## ...Privacy and Confidentiality

- **Your Supervisor/Manager**
- **Privacy Office:** (310) 835-7135  
**Chief Privacy Officer:** Carole A. Klove, RN, JD  
**Email:** [cklove@mednet.ucla.edu](mailto:cklove@mednet.ucla.edu)
- **HIPAA website:** <http://pmo.mednet.ucla.edu/>
- **UCLA HIPAA Research:** <http://oprs.ucla.edu/human/forms/HIPAA>
- **UCOP HIPAA website:** <http://www.universityofcalifornia.edu/hipaa>

## ...Information Security

- **Your Supervisor / Manager**
- **Your department's IT or CSC person**
- **HIPAA Website:**  
<http://pmo.mednet.ucla.edu/>
- **UCLA Medical Sciences Information Security Officer:**  
**Ann S. Chang**  
[achang@mednet.ucla.edu](mailto:achang@mednet.ucla.edu)  
**(310) 825-7003**



## HIPAA Security Reminders

- |                                      |                        |
|--------------------------------------|------------------------|
| √ Password protect your computer     | √ Keep disks locked up |
| √ Backup your electronic information | √ Run anti-virus       |
| √ Send email securely                | ○ Anti-spam software   |
| √ Keep office secured                | ○ Anti-spyware         |