HIPAA 101
Privacy and Security Training

Privacy and Security Training

Privacy and Security for New UCSF Workforce

- Faculty
- Post Docs
- Residents / Fellows
- Staff
- Students
- Trainees
- Volunteers
- Contractors / Vendors
Course Objectives

- Understand the requirements of the federal HIPAA/HITECH regulations, state privacy laws, and University policies and procedures that protect the privacy and security of confidential data and what information must be protected.
- Understand how these affect you and your job and how you can protect confidential and sensitive information.
- Understand your responsibilities for good computer practices.
- Provide instructions to report privacy breaches and security incidents.
Privacy and Security
Laws and University Policies

This section explains the following laws and policies:

- Federal HIPAA
- Federal HITECH Act
- HIPAA Final Omnibus Rule
- California Medical Information Act (CMIA)
- UC & UCSF policies and procedures
- Fines and penalties

© 2013 The Regents of University of California
All Rights Reserved
The Regents of the University of California accepts no liability of any use of this presentation or reliance placed on it, as it is making no representation or warranty, express, or implied, as to the accuracy, reliability, or completeness of the presentation.
What is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) is a federal law that requires UCSF to:

- Protect the privacy of patient information
- Secure patient health information (physically and electronically)
- Adhere to the “minimum necessary” standard for use and disclosure of patient health information
- Specify patients’ rights for access, use and disclosure of their health information
HITECH and Omnibus Updated HIPAA

The Health Information Technology for Economic and Clinical Health (HITECH) Act and the HIPAA Final Omnibus Rule updated the federal HIPAA privacy and security standards.

Collectively, major updates include:

• Breach notification requirements
• Fine and penalty increases for privacy violations
• Patient right to request electronic copies of the electronic health care record
• Patient right to restrict disclosure to health plans for services self-paid in full (“self-pay restriction”)
• Mandates that Business Associates are directly liable for compliance with HIPAA provisions
California Medical Information Act (CMIA)

- Apply to individuals as well as institutions
- Unauthorized access includes the inappropriate review or viewing of patient medical information without a direct need for diagnosis, treatment or other lawful use
- Licensed facilities, like UCSF Medical Center, are required to report incidents of unauthorized access, use, or disclosure of medical information to the California Department of Public Health, and to the affected patient within 5 business days after breach detection
- When you suspect or know of a breach you must report it to the Privacy Office immediately
  - Medical Center employees must also submit an Incident Report
Privacy is bigger than HIPAA

- **Other Federal Laws**
  - Medicare Conditions of Participation promoting patient rights including privacy
  - Federal Trade Commission protection of consumer privacy
  - FERPA protection of student education records
  - HHS and multiple agencies’ protection of information

- **Other California State Laws**
  - Confidentiality of Medical Information Act (CMIA)
  - Title XXII protections of patient records
  - Information Practice Act
  - Breach notifications
  - Lanterman-Petris-Short (LPS) protection of mental health records

- **University Policies and Procedures**

- **Refer to the UCSF Privacy and Confidentiality Handbook for further guidance**
University of California and UCSF

- UC and UCSF have policies and procedures to protect the privacy and security of information.
- As a UCSF workforce member, **you are responsible** to follow these policies and procedures to protect the privacy and security of information.
- Ask your Supervisor or Manager for guidance.
- Remember that privacy applies to ALL verbal, written, and electronic information.
Fines and Penalties

Privacy violations may carry penalties under federal HIPAA/HITECH, state privacy laws, and UC policies:

- HIPAA Civil Penalties
  - $100 - $1,500,000 / year fines
  - More fines if multiple year violations

- HIPAA Criminal Penalties
  - $50,000 - $250,000 fines
  - Imprisonment up to 10 years

- State Laws
  - Fines and penalties apply to individuals as well as health care providers, up to a maximum of $250,000; may impact your professional license
  - Imprisonment up to 10 years

- UCSF corrective and disciplinary actions
  - Up to and including loss of privileges and termination of employment
  - Refer to Campus Policy 200-32, “Workforce Sanctions for Patient Privacy Violations”
How the Laws Affect You and Your Job

This section explains:

• How the privacy laws apply to you
• Who uses PHI at UCSF
How the HIPAA Laws Apply to You

HIPAA requires that UCSF train its **workforce members** about the University’s HIPAA policies and specific procedures which may affect the work you do. These rules apply to you when you look at, use, or share Protected Health Information (PHI).
Who Uses PHI at UCSF?

• Anyone who works with or may view health, financial, or confidential information with HIPAA protected health identifiers

• Everyone who uses a computer or electronic device which stores and/or transmits information

• The following workforce members:
  o All Medical Center staff
  o Faculty Group Practice staff
  o Schools of Medicine, Nursing, Dentistry, Pharmacy: staff and faculty
  o Campus staff who work in clinical areas
  o Administrative staff with access to PHI
  o Volunteers
  o Students who work with patients
  o Clinical researchers and staff investigators
  o Billing and accounting staff
  o Almost EVERYONE, at one time or another
Protected Health Information (PHI)

This section explains:

• What information must be protected
• PHI identifiers
• UCSF’s use or disclosure of PHI
• The Notice of Privacy Practice (NPP) for PHI
• Examples of Treatment, Payment, or Operations (TPO)
• Purposes other than TPO
• Exceptions to the “Minimum Necessary” standard
• HIPAA patient rights
• Use of social media
• Guidelines for viewing, using, or sharing PHI
What Information Must Be Protected?

You must protect an individual’s PHI which is collected or created as a consequence of a health care provision.

- PHI:
  - Information related to a patient’s past, present or future physical and/or mental health or condition
  - Includes at least one of the 18 personal identifiers (see next slide)
  - In any format: written, spoken, or electronic (including videos, photographs, and x-rays)

- PHI includes health information about individuals who have been deceased less than 50 years

- These rules apply every time you view, use, and share PHI
Protected Health Information (PHI) Identifiers

The **18 Identifiers** Defined by HIPAA are:

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

© 2013 The Regents of University of California
All Rights Reserved
The Regents of the University of California accepts no liability of any use of this presentation or reliance placed on it, as it is making no representation or warranty, express, or implied, as to the accuracy, reliability, or completeness of the presentation.
In order for UCSF to use or disclose PHI:

- UCSF must give each patient a **Notice of Privacy Practice** (NPP) that:
  - Describes how UCSF may use and disclose PHI
  - Advises the patient of his/her privacy rights

- UCSF must attempt to obtain the patient’s signature acknowledging receipt of the Notice, except in emergency situations. If a signature is not obtained, UCSF must document the reason why.
Notice of Privacy Practice for PHI

The NPP allows PHI to be used and disclosed for purposes of TPO

- Treatment (T), Payment (P), Operations (O)
  - TPO includes teaching, medical staff/peer review, legal, auditing, quality reviews, customer service, business management, and releases mandated by law
  - UCSF must have a Business Associate Agreement (BAA) with vendors who will access or use PHI when providing a service to UCSF

© 2013 The Regents of University of California
All Rights Reserved
The Regents of the University of California accepts no liability of any use of this presentation or reliance placed on it, as it is making no representation or warranty, express, or implied, as to the accuracy, reliability, or completeness of the presentation.
Examples of TPO

- The patient’s referring physician calls and asks for a copy of the patient’s recent exam at UCSF (Treatment)
- A patient’s insurance company calls and requests a copy of the patient’s medical record for a specific service date (Payment)
- The Quality Improvement office calls and asks for a copy of an Operative Report (Health Care Operations)
- For these TPO purposes, patient information may be provided
- **Unsure as to what constitutes TPO? Just ask your Manager or the Privacy Office!**
Purposes Other Than TPO

Unless required or permitted by law, UCSF must obtain written authorization from the patient to access, use or disclose their information.

- **Patient Authorization** allows UCSF to disclose information for purposes not related to treatment, payment, or operations
  - Exception: Final Omnibus Rule provided greater flexibility to release child immunization records to schools where state law requires them to have proof of immunization (e.g., California schools). While you still need to obtain parental agreement to disclose the records, this agreement can be verbal or written; verbal agreement must be documented in the patient’s record.

- For **Human Subjects Research**, additional rules and training apply (see Committee for Human Research website guidance at http://www.research.ucsf.edu/chr/HIPAA/chrHIPAA.asp)
  - PHI may not be accessed for human subjects research unless
    - The Committee for Human Research (CHR) has approved the research and
    - **BOTH** Informed Consent and HIPAA Authorization have been obtained from the subject, OR CHR has approved a Waiver of HIPAA Authorization

- **NOTE:** if you obtain or use PHI for research purposes with only an Informed Consent but without a HIPAA Authorization, it is considered an unauthorized disclosure under HIPAA.
If you are involved in **fundraising**, additional rules apply:

- Review Policy 450-10 Authority to Solicit Funds through Gifts, Private Grants and Events at [http://policies.ucsf.edu](http://policies.ucsf.edu)
  - PHI may not be **accessed, used or disclosed** for fundraising without prior **written authorization**
  - Only a patient’s healthcare provider may request that the patient sign the Authorization
  - Authorizations must be forwarded to UCSF’s Development and Alumni Relations (UDAR) office
  - UCSF policy requires coordination with UDAR for all fundraising efforts that target patients
  - Contact UDAR for fundraising-related questions at [giving@support.ucsf.edu](mailto:giving@support.ucsf.edu)
Except for Treatment, the **Minimum Necessary Standard Applies**

- For patient care and treatment, HIPAA does not impose restrictions on use and disclosure of PHI by health care providers
  - Exceptions: *psychotherapy* information, *HIV* test results, and *substance abuse* information

- For other purposes, HIPAA requires users to access the minimum amount of information necessary to perform their duties
  - Example: a billing clerk may need to know what laboratory test was done, but not the result
HIPAA Gives Patients Specific Rights

- Right to **access** and **receive a copy** of one’s own PHI (paper or electronic formats)
- Right to request **amendments** to information
- Right to request **restriction** of PHI uses and disclosures
- Right to restrict disclosure to health plans for services self-paid in full (“**self-pay restriction**”)
- Right to request **alternative forms of communications** (mail to P.O. Box not street address; no message on answering machine, etc.)
- Right to an **accounting of the disclosures** of PHI
Use of Social Media

• Do not share on social media any patient information acquired through your work at UCSF, even if the information is public

• Information obtained from your patient/provider relationship is confidential

• Posting patient information without authorization is a violation of the patient’s right to privacy and confidentiality

• Even if you think you’ve de-identified the information, it still might be identifiable to others

• NOTE: De-identification of PHI requires removal of all 18 PHI identifiers, which includes “Any other unique identifying number, code, or characteristic” (e.g., photo of a wound; description of a patient’s condition)

• Refer to UCSF’s Social Media Best Practices: http://www.ucsf.edu/about/social-media-overview/social-media-best-practices
When Is It Appropriate To?

- View PHI
- Use PHI
- Share PHI

Only when required for your job.
Remember – It’s Common Sense

- Use information **only when necessary** to perform your job duties
- Use only the **minimum necessary** to perform your job duties
- Follow UCSF Medical Center and UCSF campus policies and procedures for information confidentiality and security
- Ask your supervisor for your department’s privacy and security procedures
Scenario 1

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

A. You may not discuss any patient information with anyone unless required for your job
B. You may only talk about the patient with your coworkers
C. You may only talk about the patient with your family and friends
Scenario 1 - Answer

The correct answer is A.

Information can only be used as needed for your job.

A. You may not discuss any patient information with anyone unless required for your job
B. You may only talk about the patient with your coworkers
C. You may only talk about the patient with your family and friends

© 2013 The Regents of University of California
All Rights Reserved
The Regents of the University of California accepts no liability of any use of this presentation or reliance placed on it, as it is making no representation or warranty, express, or implied, as to the accuracy, reliability, or completeness of the presentation.
Scenario 2

My co-worker’s husband notified me that my co-worker was recently admitted to the Emergency Department and won’t be coming into work tomorrow. My co-worker and I have a great relationship, and I’d like to know how she’s doing. May I access her records to check on her condition?

A. It is okay as we are friends, so I’m sure she wouldn’t mind me looking at her records.

B. I already have approval to access patient clinical systems, so no one will know that I accessed it.

C. It is not necessary for my job, so I would be violating the patient’s privacy by accessing her records. I should contact her husband to check on her condition.
Scenario 2 - Answer

The correct answer is C.

It is not part of your job – your access to your co-worker’s record would be for personal reasons. Therefore, accessing the record will be a violation of your co-worker’s privacy. Furthermore, your access to the record will automatically be recorded and tracked. There could be serious consequences to your employment.

A. It is okay as we are friends, so I’m sure she wouldn’t mind me looking at her records
B. I already have approval to access patient clinical systems, so no one will know that I access it
C. It is not necessary for my job, so I would be violating the patient’s privacy by accessing her records. I should contact her husband to check on her condition
Scenario 3

You are very upset because a young patient of yours has just coded and was not able to be resuscitated. You want to share this experience and your thoughts and feelings with your family and friends on Facebook. What must you consider before doing this?

A. Posting this on Facebook is OK as long as you do not identify the patient by name, or identify the hospital, and you are limiting the recipients to your friends and family

B. You cannot post anything on Facebook that could possibly lead to identification of the patient
Scenario 3 - Answer

The correct answer is **B**.

- **Facebook** is considered public domain, and anything you post there is considered public information.
- Posting clinical details without prior authorization is a violation of your patient’s privacy and confidentiality.
- Your Facebook profile may identify your place of work and your occupation. When linked with your posting, and with any other publicly available information, the additional details may identify the patient.
- Information you obtain from your patient/provider relationship is confidential.

**A.** Posting this on Facebook is OK as long as you do not identify the patient by name, or identify the hospital, and you are limiting the recipients to your friends and family.

**B.** You cannot post anything on Facebook that could possibly lead to identification of the patient.
Protecting Privacy

This Section Explains:

- Verbal exchanges
- Knowing where you left your paperwork
- Taking PHI offsite
- Disposal of paper documents
- Privacy breaches from lost, stolen, or misdirected information
- Examples of privacy breaches
Verbal Exchanges

- Patients may see normal clinical operations as violating their privacy
- Be aware of your surroundings when talking
- Do not leave PHI on answering machines
- Ask yourself, “What if my information was being discussed like this?”
Know **Where You Left Your Paperwork**

- **Double check!!** When mailing or handing documents to patients/family members, slow down and verify that each document belongs to the patient.

- Check printers, faxes, and copier machines when you are done using them.

- Do not leave paper PHI laying on your desk; lock it up at the end of the day.
Taking PHI Offsite Involves Risk

• Theft and loss of PHI is a high risk
  – Your car is burglarized and the thief takes off with the PHI (*this happens very often, especially in San Francisco*)
  – Leaving PHI in a coffee shop, restaurant or public transportation

• If your job requires you to work from home or transport PHI between sites, follow best practices:
  – Access PHI remotely via Virtual Private Network (VPN)
  – Securely fax or email the PHI to yourself and securely access it from the offsite location to avoid carrying PHI
  – Ensure all devices used to access ePHI or UCSF email are encrypted (including your personal laptop, iPad, iPhone, etc.)
  – Never leave PHI unattended in your bag, briefcase or your car (even if it’s locked in the trunk!)

• This applies to all types of PHI – paper, films, photos, cameras, CDs and ePHI stored on laptops

• *Treat PHI like it’s an infant: You are responsible for securing and keeping it in your possession at ALL TIMES*

© 2013 The Regents of University of California
All Rights Reserved
The Regents of the University of California accepts no liability of any use of this presentation or reliance placed on it, as it is making no representation or warranty, express, or implied, as to the accuracy, reliability, or completeness of the presentation.
Disposal of Paper Documents

• Shred or destroy PHI before throwing it away

• Dispose of paper and other records with PHI in secure shred bins. Recycling and trash bins are NOT secure.

• Shred bins only work when papers are put inside the bins. When papers are left outside the bin, they are not secure from:
  ▪ Gossip
  ▪ Daily regular trash pickup
  ▪ The public
Privacy Breaches from Lost, Stolen, or Misdirected Information

A privacy breach can occur when information is:

• Physically lost or stolen
  ▪ Paper, films, cameras, CDs, electronic devices
  ▪ Anytime, anywhere - even on public transportation, crossing the street, in the building, in your office, in your car, at a restaurant

• Misdirected to others outside of UCSF
  ▪ Verbal messages left for the wrong person
  ▪ Misdirected mail or email
  ▪ Wrong phone or fax number
  ▪ Posted to UCSF intranet, internet, websites, Facebook, Twitter
  ▪ Incorrect use of or failure to use UCSF’s secure email
Examples of Privacy Breaches

- Talking in public areas, talking too loudly, talking to the wrong person
- Lost/stolen or improperly disposed paper documents, films, notebooks, medication bottles
- Lost/stolen unencrypted laptops, tablets, cell phones, media devices (video and audio recordings)
- Lost/stolen unencrypted zip disks, CDs, flash drives, memory sticks
- Hacking of unprotected computer systems
- Email or faxes sent to the wrong address, wrong person, or wrong number
- Users not logging out of computer systems, allowing others to access their computer or system
Scenario 4

I called a patient’s phone number and left a voice mail for Mr. John Smith to contact UCSF regarding his scheduled thyroid surgery. Was this a privacy breach?

A. No, the patient provided this phone number
B. Potentially, I stated his name and medical procedure
C. No, I did not state the medical reason for the surgery
Scenario 4 - Answer

The correct answer is B.

Patient name in conjunction with medical information constitutes PHI. You do not know who will hear the message; the patient may not have told his family, friend or roommate. It is best practice to leave the minimum amount of information needed: your name, phone number, and that you are from UCSF. Never leave PHI on an answering machine. Ask your supervisor for the voice mail procedure in your area.

A. No, the patient provided this phone number
B. Potentially, I stated his name and medical procedure
C. No, I did not state the medical reason for the surgery
Your Responsibilities for Good Computing Practice

This section explains:

• Security of ePHI
• Power of encryption
• Computer security
• Safe emailing
• Additional security precautions
Security of Electronic Patient Information (ePHI)

Good security standards follow the “90/10” Rule:

- 10% of security safeguards are technical
- 90% of security safeguards rely on the user (YOU) to adhere to good practices
Security of ePHI – Recent Headlines

Ever evolving technology brings opportunities and efficiency – but only when managed properly. Consider these recent headlines:

October 2013 – An academic medical center notified 3,541 patients that their ePHI was compromised after the theft of an unencrypted personal laptop.

June 2013 – A healthcare organization notified 13,000 patients that their ePHI was compromised after the theft of an unencrypted laptop.

September 2012 – A healthcare organization agreed to pay the U.S. Department of Health and Human Services $1.5 million to settle HIPAA violations after the theft of an unencrypted personal laptop, containing ePHI of ~3500 patients and research subjects.

How could these incidents have been avoided? By **encrypting** the device.
Do you use your personal device (e.g., laptop, iPhone, iPad, external hard drive) for UCSF business?

**Hint:** This includes checking your UCSF email from your personal device.

Even if you don’t intentionally save PHI onto your device, your UCSF email files may download to your device without your knowledge.
Power of Encryption

If you use your device for UCSF business, it **MUST BE ENCRYPTED!!**

- Encryption is the only federally recognized method for securing ePHI.
- By having your device encrypted, you can rest assured that the information it contains is secure and inaccessible to others if the device is lost or stolen.
- For assistance with encryption, contact the IT Service Desk at (415) 514-4100.
- You may need to attest annually that all of your devices used for UCSF business are encrypted.

**Best Practice:** Do not use your personal device to store UCSF data or access UCSF email unless absolutely necessary. And if necessary, the device must be encrypted.

© 2013 The Regents of University of California
All Rights Reserved
The Regents of the University of California accepts no liability of any use of this presentation or reliance placed on it, as it is making no representation or warranty, express, or implied, as to the accuracy, reliability, or completeness of the presentation.
Computer Security

- Ensure your computer is physically secured by using lockdown cables, locked drawers, placement in a secured area, etc.

- Never leave your laptop unattended in your vehicle or bag

- Create a strong password and do not share your username or password with anyone

- Log off or lock your computer when done, and every time you walk away

- Ensure information on computer screens is not visible to passersby
  - Consider a privacy screen
  - Lock your PC by using the keyboard command Ctrl + Alt + Delete
  - Use a password to start up or wakeup your computer

- Ensure your system has anti-virus and all necessary security patches and updates

- UCSF IT website: http://it.ucsf.edu/
How to Send UCSF Emails Securely

• Secure your UCSF email message by starting the subject line with one of the following trigger words:
  ▪ ePHI:
  ▪ PHI:
  ▪ Secure:

• Correct spelling and use of the colon is important

• Trigger words are not case-sensitive

• Detailed instructions are available at: http://it.ucsf.edu/services/secure-email/tutorial/how-secure-email-works
When to Use Secure Email

• Use secure email when emailing PHI outside of UCSF, such as emails to:
  ▪ Patients
  ▪ Vendors
  ▪ Any non-UCSF email address

• Best practice: Use MyChart to electronically communicate with patients

• If a patient doesn’t want to receive secure emails, and requests unencrypted email communications, you must do the following before honoring the request:
  – Notify the patient of the risks of sending unencrypted emails
  – Document the patient’s preference for unsecured email in the patient’s record

© 2013 The Regents of University of California
All Rights Reserved
The Regents of the University of California accepts no liability of any use of this presentation or reliance placed on it, as it is making no representation or warranty, express, or implied, as to the accuracy, reliability, or completeness of the presentation.
Additional **Security Precautions**

- Make sure your computer has anti-virus and all necessary security patches. UCSF Medical Center IT automatically updates these weekly. Do not interrupt these updates! You can continue to work while they are being installed.

- Do not install unknown or unsolicited programs

- Practice **Safe Emailing**
  - Do not open, forward, or reply to suspicious emails
  - Do not open suspicious email attachments or click on unknown website addresses
  - **NEVER** provide your username and password to an email request
  - Delete spam and empty the “Deleted Items” folder regularly

- It is **your responsibility** when communicating to send all PHI securely
Scenario 5

As part of my job, I need to use a laptop for my work at various UCSF sites. I have patient emails, addresses, and medical information on the laptop. What is the best way to protect this device?

A. The information on my portable device is encrypted, I use a complex password, and I physically secure the device when leaving it unattended
B. I only need a complex password to secure the laptop
C. It is secured as I use a complex password and when unattended, I always lock it up in the trunk of my car
D. None of the above
Scenario 5- Answer

The correct answer is A.

Your laptop must be **encrypted** if it contains UCSF patient information or other sensitive confidential information. Password protection by itself is not enough, but you do need to use complex passwords, keep it with you during transport and physically secure it when unattended. Unencrypted devices are considered unsecure in the event of a loss or theft, and therefore reportable to federal and state agencies!

A. The information on my portable device is encrypted, I use a complex password, and I physically secure the device if leaving it unattended

B. I only need a complex password to secure the laptop

C. It is secured as I use a complex password and when unattended, I always lock it up in the trunk of my car

D. None of the above
Scenario 6

I have a personal laptop at home, which I sometimes use to check my UCSF email on the weekends. However, I never save files containing PHI onto my laptop. Does it still need to be encrypted?

A. No, because I rarely use my personal laptop for UCSF business
B. Yes, because I access my UCSF email, which may result in files automatically downloading to my laptop, without my knowledge
C. No, because I don’t save files containing PHI on my laptop
Scenario 6 - Answer

The correct answer is B.

Your laptop must be **encrypted**. Accessing UCSF email from your personal laptop may result in your UCSF data, mail and attachments being automatically downloaded and stored on your device. Therefore, it is important that you encrypt your personal device before using it for UCSF business.
If the device is lost or stolen, the information in it (both your personal and UCSF information) is secure and inaccessible to thieves.

A. No, because I rarely use my personal laptop for UCSF business
B. Yes, because I access my UCSF email, which may result in files automatically downloading to my laptop, without my knowledge
C. No, because I don’t save files containing PHI on my laptop
Scenario 7

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

A. It is a physician, so it is okay to do this
B. Ignore the request and hope he forgets
C. Decline the request and refer him to the UCSF Information Security Policies
D. None of the above
Scenario 7 - Answer

The correct answer is C.

Always login with your own user ID and password. If you do not have system owner permission to access the system, then do not access the system. Doing so would be a violation of UCSF privacy and security policies.

A. It is a physician, so it is okay to do this
B. Ignore the request and hope she/he forgets
C. Decline the request and refer them to the UCSF information Security Policies
D. None of the above
Remember

You are responsible for using the following workstation security safeguards:

• Protecting your user ID
• Protecting your password
• Logging out of programs that access PHI when not in use
How to Report Privacy Breaches

**Immediately** report any known or suspected privacy breaches to the Privacy Office at (415) 353-2750.
How to Report Security Incidents

• Immediately report lost or stolen electronic devices (e.g., laptops, smart phones, mobile devices, flash drives) to the UCSF Police Department at (415) 476-1414 (even outside of business hours or if you are overseas)

- Immediately report any unusual or suspected information security incidents (including but not limited to the loss and/or theft of any form of ePHI, as well as unusual computer activity) to your Supervisor and/or your department’s IT or Computing Support Coordinator (CSC)

• If no one is available to receive your report, contact IT Service Desk at (415) 514-4100

• You can also go to the UCSF website: http://it.ucsf.edu/security
Importance of **Immediate** Reporting Of Known or Suspected Incidents

State law requires that unauthorized access, use or disclosure of patient medical information be reported within 5 working days of detection of the breach to the CA Department of Public Health, and the affected patient(s) or their legal representative.
Remember

To the patient, **ALL** information is private.

- This includes a patient’s:
  - Personal information
  - Financial information
  - Medical information
  - Protected Health Information
  - Information in any format: spoken, written, or electronic
Remember

Protect patient information by:

- Protecting verbal, written, and electronic information
- Utilizing safe computing skills
- Reporting suspected privacy and security incidents
- Following University policies
- Asking for help if you are unsure
Resources for Privacy and Security

• Your Supervisor/Manager
• Your Department’s IT or Computer Support Coordinator (CSC)
• Privacy Office
  ▪ (415) 353-2750
  ▪ Chief Privacy Officer: Deborah Yano-Fong
• UCSF Information Security Officer: David Rusting
• UCSF Medical Center Information Security Officer: Rob Winter
• Online Resources:
  ▪ UCSF Privacy Website: http://hipaa.ucsf.edu
  ▪ UCOP HIPAA Website: http://www.universityofcalifornia.edu/hipaa
  ▪ HIPAA and Research Website: http://www.research.ucsf.edu/chr/index.asp
  ▪ UCSF Security Awareness and Training Website: http://awareness.ucsf.edu
Next Steps

To receive credit for completing the HIPAA 101 Privacy and Security Training, you MUST:

2. Sign the Acknowledgement of Responsibility
3. Provide the Signed Acknowledgement to your Supervisor

The Statement of Privacy Laws and University Policy can also be obtained from your Supervisor.