

# Advanced HIPAA Security Training Module

## *The Security of Electronic Information*

Copyright 2008 The Regents of the University of California

All Rights Reserved

The Regents of the University of California accepts no liability for 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.

# Purpose of the Training

- ◆ Raise awareness about how each member of the UCSF community can protect **UCSF patients'** confidential, electronic information and:
  - Better **understand the risks** when using and storing electronic information
  - Better **understand how to reduce the risks** to the confidentiality, integrity and availability of confidential, electronic information

# HIPAA **Advanced** Security Training Is For...


- Faculty, students, staff, trainees, and volunteers who create, receive, transmit, access, or store **confidential** UCSF electronic information, including
  - ◆ **Emails** containing confidential UCSF health or financial data
  - ◆ Confidential data on portable, **wireless, mobile media.**

# Advanced HIPAA Training

- ◆ Why now?
- ◆ What is confidential, electronic information, including Electronic Protected Health Information (ePHI)?
- ◆ Why me?
- ◆ What do I need to do to protect confidential, electronic information?
- ◆ How do I get help?

# Why Now?

- ◆ Recent UC, state and national incidents demonstrate that the **theft of electronic data and devices is exploding**
  - Threatens the confidentiality of everyone's data—yours, mine, UCSF's patients and research subjects
- ◆ **Federal and State Law and UC Policy** require us to know how to secure information
  - **HIPAA Security Rule** mandates Security Awareness Training
  - State law **SB 1386** (requires notification if there is a suspected incident involving unencrypted data with Social Security Numbers and other personal identifiers)
  - **UC and UCSF policies** require an understanding of electronic security safeguards



UCSF needs **your help** to  
implement safeguards to  
protect confidential  
information

# What Electronic Information Is Covered by This Training and UC Policy?

...all information that is  
**confidential**

...including **electronic Protected  
Health Information (ePHI)**  
covered by the HIPAA Security Rule

# Confidential Electronic Information is...

- ◆ “Information that may or may not be protected by law but which is desired to be treated as confidential and protected as such.”  
UCSF Policy 650-16; UCSF Medical Center Policy 5.01.04
- ◆ “Access to confidential information is prohibited unless permitted by policy or an exception to the law.” UCSF Policy 650-16; UCSF Medical Center Policy 5.01.04
- ◆ All reference to “Confidential Electronic Information” in this training **includes Electronic Protected Health Information (ePHI)**

# Electronic Protected Health Information (ePHI)\* is:

- ◆ An individual's **health or financial information** that is **used, created, received, transmitted or stored** by UCSF using any type of electronic information resource
- ◆ Information in an electronic medical record, patient billing information transmitted to a payer, digital images and print outs, information when it is being sent by UCSF to another provider, a payer or a researcher
- ◆ For example: An **unsolicited email message** from a patient after it is received by the healthcare provider or UCSF

**\*ePHI is used in the HIPAA Security Rule to describe information that must be secured**

# All References to Your Computer Workstation Include:

- ◆ Traditional, PC/desktop computer workstations at UCSF, at home or in an off-site lab
- ◆ Laptops at UCSF, home, or in an off-site location, including use in a wireless cafe, hotels, lecture halls
- ◆ All other mobile, wireless devices such as Blackberries, PDAs, memory sticks, etc., that allow you to use, create, receive or transmit confidential, electronic information
- ◆ A computer workstation that is UCSF-owned or has been provided by UCSF
- ◆ A computer workstation that you have purchased or own

# The HIPAA Security Rule Applies to Your Use of...

- ◆ A computer workstation “on-site” at UCSF or a UCSF facility
- ◆ A UCSF-provided computer workstation “off-site” at home, in a cafe, on a plane, in a hotel, etc.
- ◆ The use of your own, non-UCSF computer workstation, laptop or mobile device for UCSF activities using ePHI or other confidential information

***You Are Responsible for Your Actions With  
Confidential UCSF Information***

# Why Me?

...**You use**

a UCSF computer workstation to do  
your job

...**Each of us**

**is responsible** for understanding and  
reducing the risks to confidential,  
electronic information

# Q: I'm a UCSF Researcher...Do I Need Training?

A: If the electronic information that you use were **lost, stolen, changed, or misused by others...**

- Could you restore or recreate the data?
- What if the data were in emails?
- How long did it take you to obtain the electronic data stored on your laptop?
- How many years of field research?
- Could you continue to do your job?
  - ◆ Your basic sciences research?
  - ◆ Teaching activities?
  - ◆ Business functions?

# Ask Yourself...

- ◆ **Should I take the risk** of a significant loss of my professional reputation, my time, and the costs of recovering this information?

***OR***

- ◆ **Should I take the time** now to implement reasonable and appropriate safeguards?

# Information Technology Alone Is Not the Answer to Securing Information...

**Each one of us is responsible**  
for safeguarding her/his  
computer workstation and  
confidential information,  
including ePHI

What Do I Need to Do to  
Protect **ePHI** or Other  
Confidential UCSF  
Information?

# First, Identify the Risks At Your Computer Workstation, Including:

- ✓ Failure to use passwords or your unique user ID
- ✓ Use of weak or shared passwords
- ✓ Failure to use a protected screen saver or similar protective feature
- ✓ Failure to logoff after each use
- ✓ Use of unlicensed software
- ✓ Failure to run virus scans or install anti-viral software
- ✓ Failure to install personal firewalls
- ✓ Physical access by individuals who should not have access to your computer, laptop or confidential data on your workstation
- ✓ Can you think of others?

# Control Access to Electronic Information at Your Workstation

- ◆ Create a “Layered Defense” for your computer-- install and use:
  - Strong Passwords and unique user ID
  - Protected screen saver or other automatic log-Off
  - Anti-virus software, including virus scans
  - Personal firewall software

# First Line of Defense: Strong Passwords

- ◆ Use **strong Passwords** that are hard to guess, easy to remember and change them often
- ◆ Use a mixture of **at least 7** letters, symbols, numbers, and capital letters
- ◆ Think of designing a **car "vanity plate"** to help create a Password unique to you

# Protect Your Passwords and Unique User ID

- ◆ You are responsible for actions taken with your Password and ID
- ◆ Do NOT post, write or share Passwords with ANYONE (e.g., not your IT systems manager, colleague, friend, or boss)
- ◆ Protect your user ID and Password from fraudulent use, unethical behavior, or irresponsible actions by others—don't let someone "be you" and use your password for illegal behavior!

# Prevent Unwanted Access

- ◆ **Just say "NO"** when the program asks:  
"Do you want me to remember your password?"
  - When the password is saved on your hard drive, it makes you and your data vulnerable to hackers who could steal your Password
- ◆ Always **log off** shared workstations
  - If you don't log off, someone else could use your ID to illegally access confidential information

# Control Physical Access to Your Computer Workstation

- ❖ Only authorized UCSF users should have **physical access** to your workstation, including your laptop, mobile or wireless device
- ❖ **You are responsible** for physically securing and protecting the device and any confidential information
  - ❖ Use Passwords and log-off
  - ❖ Lock the computer and lock the door to the office
  - ❖ Don't leave portable devices unattended, even for a moment
- ❖ Immediately **report unusual incidents**, including access by people who do not have UCSF identity badges

# Viruses Are Becoming More Lethal and Sophisticated...

- **NEVER** open an email attachment, unless you know who sent it and why
  - If in doubt, call the sender of the email to confirm that the attachment is safe and valid
- **ALWAYS** run an updated antivirus tool
  - DO NOT cancel the scheduled virus scan
- **NEVER** load software that you or your department are not licensed to use on a UCSF workstation
- **ALWAYS** close “pop-ups” when they solicit a response to advertisements or other messages
  - Click the “x” box to close the pop-up ad
  - Clicking “no” is the same as “yes” and allows the virus or hacker access to your computer

# Be Aware: Email is **NEVER** 100% secure

- ✓ **Avoid** using email to send, receive or store confidential information critical for UCSF business, research, or training
- ✓ **Never use** a non-UCSF mail account (e.g., Yahoo, AOL, etc.) **to initiate or start** an email communication that you want to protect
  - ✓ You could be exposing UCSF confidential information to an unprotected, risky transmission
  - ✓ The secure email solution will not secure these transmissions

# If You Use Email to Receive or Transmit Confidential Information

- ◆ You must use the **UCSF secure email** solution OR the **alternative secure solution** offered by your department
  - The secure solution should encrypt, at minimum, all outbound transmissions
- ◆ The secure email solution is available to the three major email exchanges: Medical Center, SOM and ITS
  - **Contact your departmental computer support** resource or department manager to find out if you have secure email

# The UCSF Secure Email Solution

For the three major email exchanges—i.e., Medical Center, ITS, and School of Medicine, UCSF has implemented a **secure email solution** that will reasonably secure outbound communications, including faculty to patient

- a. In general, when using a **UCSF address**, you will be able to communicate with your patient if you are using the secure email solution
- b. **Each department is responsible** for implementing the secure email solution and instructing faculty and staff how to implement the solution
- c. If you have not received information from your departmental chair or IT resource, **you are responsible** for finding out if your outbound emails are secure

# If You Use Email For Teaching, Clinical Care, Business Activities...

- Security for email transmissions includes a number of measures, including encryption, firewalls, secure servers **AND changing the way each of us limits and protects the use of email for confidential communications**
- As technologies emerge, UCSF will employ additional measures
- Contact **IT Customer Support or your department IT resource** to learn about the actions your Department has taken to secure email transmissions

# How Do I Check Email With My Wireless Device?

- ◆ Use only an approved, secure method for accessing the UCSF network via **VPN or other means** :

*[its.ucsf.edu/services/network](https://its.ucsf.edu/services/network)*

- ◆ Go On-Line to obtain additional guidance at:

*[www.ucsf.edu/hipaa/dept\\_compliance/](http://www.ucsf.edu/hipaa/dept_compliance/)*

# Email Best Practices

◆ **Never use** a non-UCSF mail account (e.g., Yahoo, AOL, etc.) **to initiate or start** an email communication that you want to protect

The secure email solution will  
**not** secure these transmissions

# Best Practices: Transmission of Confidential Information

- ◆ Limit the confidential information to the **minimum necessary**
  - Never transmit **Social Security Numbers** unless you have used the secure email solution or another methodology for securing the transmission
- ◆ **Delete personal identifiers** when possible:
  - Name, full face, comparable images or unique identifiers
  - Dates: DOB, DOD, discharge & admission dates
  - Numbers: phone, fax, medical record, SS #, account, health plan, license or certificate
  - Biometric, vehicle license plate and device identifiers or serial numbers
  - Addresses: email, home, URLs, Internet Protocol (IP)
  - Any other unique identifiers

# Has Your Mobile Device Ever Been Stolen or Lost?

- ◆ **Act as if** someday you could lose or misplace your mobile device (laptop, Blackberry, cell-phone, digital camera)
- ◆ **Act NOW** to protect all electronic data on Mobile Devices
- ◆ **Limit** the amount of sensitive or personal information contained on the mobile or wireless

# Do You Use a Mobile Device To Store Data?

- ◆ If your Mobile Device (laptop, PDA, etc.) is your primary computer, you should have a **separate device** as a secure, backup device
- ◆ Keep the “backup” device in a **separate, secure location**
- ◆ If you use a mobile, wireless device for backup (e.g., a memory stick), then **encrypt** all sensitive data and store separately
- ◆ When available, always save and store to a **secure server** (check with Departmental Computer resource)

# Protect the Availability of Confidential Data On All Workstations

## ***Ask Yourself:***

- ✓ How often should I backup my work?
- ✓ What is the secure drive on my computer? (e.g., usually it is NOT the c-drive or your hard-drive)
- ✓ Does my department or division have a secure server?
- ✓ Do I know how to backup to a secure server?
- ✓ Could I do my job if this data were lost due to a power outage, virus, crash, etc?
- ✓ What would be the effect on patient care, business operations or my research study if this data were no longer available?
- ✓ Do I know what to do in the event of a power outage or crash?

# Always Have a Backup Plan

- ◆ **Saving to the secure server** is one of the best ways to protect the integrity, confidentiality and availability of irreplaceable, critical electronic information
- ◆ Create a **“backup” file** on a separate mobile device, including a floppy, CD or memory stick—and store the backup in a place separate from the primary computer
- ◆ **Encrypt** or otherwise protect the backup

# If You Don't Know How...

- ◆ Ask your **Department's Computer Support**, systems manager, or business manager
- ◆ **Seek help** from one of the resources listed at the end of the presentation
- ◆ **Call Customer Support** at (415) 514-4100

# Reporting Computer Security Incidents Creates Strong Security

- ✓ **Report** erratic computer behavior or unusual email messages to your department manager, dept IT resource, or IT Customer Support
- ✓ **Report** any suspected issues or incidents to a manager or the UCSF Enterprise Information Security Officer
- ✓ **Report** lost or stolen devices to UCSF Police (415) 476-1414 and, when appropriate, Local Police

# Is This a Security Incident?

- ◆ You return to your computer workstation after lunch and notice that a patient's financial record is open on the screen
- ◆ Your supervisor comments that she saw the record on the screen while you were away
- ◆ You check and determine that not only is that record accessible, but by a click one can also easily enter STOR, a medical record database, or other health care, business or research applications containing confidential information

# This is a Security Incident if

- ◆ Your passwords are weak...and there is **unauthorized access** to confidential information on a UCSF data base
- ◆ You did not log off...and confidential information was compromised **using your password and user ID**
- ◆ You suspect a problem and **fail to report the incident**


*The law requires you to implement reasonable safeguards!*

# Could This Become a Security Incident?

Dr. Gadget prides himself on being IT smart. He always uses emerging technologies for provider and patient communications. He believes this enhances his treatment and teaching activities. His newest mobile device, his Blackberry, is a mini-computer with phone, e-mail and instant-messaging. He routinely goes to the local wireless café to receive and send email communications to his colleagues and patients. The device has replaced the old-fashioned note-card, so he stores patient treatment reminders and info on this wireless device.

# What are Dr. Gadget's Potential Risks?

- ◆ Use of **email** to receive, transmit and store confidential information
- ◆ Use of a mobile device over a **wireless network** for confidential information
- ◆ Use of a **personal, mobile device** for teaching and treatment notes
- ◆ Use of **mobile media** (memory sticks, jump drive card, Secured Digital (SD) card)
- ◆ Use of a wireless cafe—a **"hot spot"**—for his "workstation"
- ◆ Can you think of **any more**?



What Should Dr. Gadget  
Have Done to Secure His  
Confidential Information?

# Dr. Gadget Should Have Understood the Risks and...

- ◆ Provided a **tracking #** for the UCSF Mobile Devices to his Department
  - UCSF can inventory all mobile devices
  - Helps the police return the lost or stolen device
- ◆ Protected **access to the data** by way of a Password or other authentication method
  - Enabled all **security features**

**Did Dr. Gadget know how to enable the Password, Virus Scan and Firewall?  
He should get help from IT Customer Support or his IT departmental resource.**

# Is This a Security Incident?

- ◆ You use a UCSF mobile, wireless device, to record and review your clinical notes
- ◆ Your car is broken into and your briefcase, containing your mobile device, is stolen

**Is this a Security Incident?**

**Are you worried that you could be held responsible for the lost or stolen device?**

# Did You Take Responsibility for Securing the Confidential Information?

- Did you protect access to the information with a unique ID and strong Password?
- Did you enable all security measures, including encryption, if available?
- Did you limit patient identifiers—particularly Social Security Numbers--to the minimum necessary?
- Did you backup the data to a secure server?
- Did you limit the amount of confidential information by deleting it ASAP?
- Did you report the loss or theft of the mobile device to UCSF Police at (415) 476-1414?

If You Can **Answer “YES”** to  
All Those Questions,

**You Took Responsibility** for  
Implementing Many of the  
Security Safeguards Required  
by Law!

# Secure Email Question # 1

- ◆ I am a teaching physician at UCSF and routinely work at home or at my local cafe and use my UCSF Blackberry to communicate w/ patients. I also want to connect with my wireless device to the UCSF network.
- ◆ Is the communication secure?

# Secure Email Question # 2

- ◆ I am a UCSF faculty physician and routinely receive emails from referring physicians that contain patient confidential information.
- ◆ Does the secure email solution protect this information?
- ◆ What is my responsibility when I receive these emails?

# Answer to Both Questions

- ◆ Protect the information as though **YOU created** the information. You must secure confidential information that you receive by email or any other electronic means --- even if you did not solicit the email.
- ◆ The secure email solution will protect the information if you **employ the solution** when you reply to the referring physician.
- ◆ Your responsibility is to **secure the email** when the data is at rest, download the information to a secure server, then delete the data from your email.
- ◆ When replying, use only the **minimum necessary**, and limit or delete personal identifiers.

# True or False

- ◆ If no reasonable effort is made by the faculty member to address the risks of email transmissions, the individual and department could be at risk of violation of HIPAA Security, HIPAA Privacy and State Law SB 1386.
- ◆ **TRUE...You are responsible for implementing appropriate and reasonable safeguards to secure the email.**

# HIPAA Requires UCSF to Tell You the Consequences for Individuals and UCSF if There is a Violation

- ◆ A violation of the Security Rule could also be a violation of the Privacy Rule and State Law
- ◆ Civil Monetary Penalties range from \$ 100 to \$ 25,000/year – more for multiple year violations
- ◆ Criminal Penalties range from \$ 50,000 - \$250,000 and imprisonment for a term of 1 to 10 years
- ◆ Fines and penalties for violation of state law, including SB 1386
- ◆ UCSF corrective and disciplinary actions, up to and including dismissal

# Understand the Law...For

## Example:

- You can not access another employee's medical records or financial information UNLESS it is specifically required by your job at UCSF
- You can not look at a patient's\* medical records or financial information UNLESS it is specifically required by your job at UCSF

***If it is not required for your job,  
it is against the law!***

**\*For example, NO friend's information  
NO celebrity patient's information**

# True or False

- ◆ Your mobile device can be safely in your pocket while your stolen, confidential information is on the Internet for all to see! (TRUE)
- ◆ There are IT solutions for assuring that your email is 100% secure. (FALSE)
- ◆ Confidential Information is a commodity in high demand! (TRUE)
- ◆ You are personally responsible for implementing safeguards that protect the confidentiality, integrity and availability of patient information on mobile devices or media. (TRUE)

# Conclusion: What Can You Do To Secure Confidential Information?

- ◆ **Take responsibility** for securing your workstation
- ◆ **Get help** from your system managers to implement IT solutions that are cost effective and meet your needs
- ◆ **Understand the laws** and procedures and seek help when requirements aren't clear
- ◆ **Report** suspected security incidents to a manager or IT Customer Support
- ◆ **Understand the consequences** of non-compliance

***AND .... HELP UCSF IMPLEMENT A LAYERED APPROACH TO THE SECURITY OF ELECTRONIC INFORMATION***

# A Layered Approach Provides a Strong Security Defense

- ◆ **Layer 1: Perimeter Defense**, includes firewalls that control harmful things that could occur on the Internet *(Example: a fence around your home or workplace, with lock or Passcode for access)*
- ◆ **Layer 2: Server Defense**, includes requiring identification and authentication of server users and assuring that current antivirus and other security patches are in place *(Example: a lock on your front door or office building with access limited to those who have a key)*
- ◆ **Layer 3: Workstation Security**, includes all of the defense mechanisms (Passcode, ID, access control, antivirus and anti-spyware, firewalls) *(Example: a lock on your bedroom door or office door, with access limited to only a few)*

# ***UCSF Is Only as Strong As Our Weakest Link!***

UCSF **needs your help** to maintain a strong defense and secure our patients' and subjects' confidential information!

# Resources and References

- ◆ Your Department's IT Resource or Support person
- ◆ UCSF IT Customer Support: 415-514-4100
- ◆ UCSF HIPAA Security Procedures, Electronic Security Policies and the HIPAA Handbook ([www.ucsf.edu/hipaa](http://www.ucsf.edu/hipaa))
- ◆ Report Suspected Security Incidents to:
  - Dept CSC, IT systems manager, business manager
  - IT Customer Support: 415-514-4100
  - UCSF Police: 415-476-1414 (lost or stolen devices)

*Thank you ...*

*...for helping UCSF create a strong, layered defense that will enhance the security of Confidential Information.*

*You have completed the Advanced HIPAA Security Training.*