



Laptops/ Mobile Device Security Issues Overview

Palm Pilots / PDAs / Cell Phones/ Blackberries, Memory Sticks
Laptops, Cameras, etc



Security Awareness By ITS-EIS SATE Program

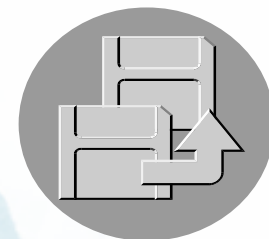
For additional information, contact Tiki Maxwell, SATE Manager at tmaxwell@its.ucsf.edu or 514-1364



Purpose of the Training

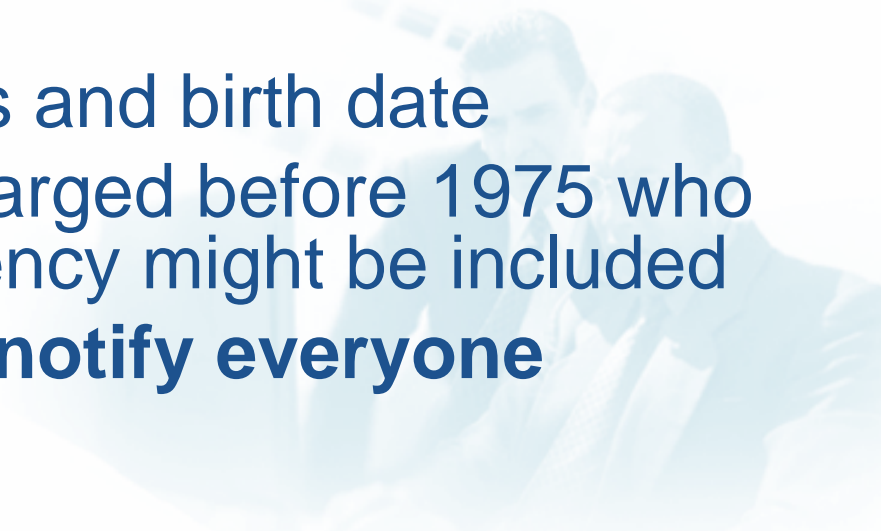
- Raise awareness about how each of us can protect **UCSF's** confidential and sensitive information (includes electronic information) and **our own personal** information
- Better understand the risks when using laptops and other mobile devices and storing information on them
- Better understand how to reduce those risks

What do mobile devices look like? Do I Have one?





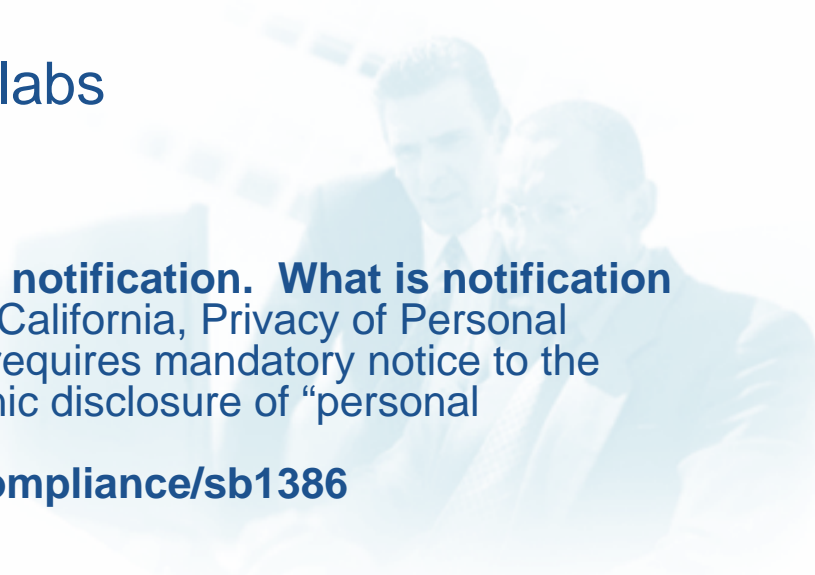
Real story in the news

- 15 May 2006 – 26.5 million veterans personal information was stolen from VA employee stolen laptop
 - An employee who had taken the information without authorization
 - the laptop contained a database of over 26.5 million Veterans names
 - Social security numbers and birth date
 - Data on veterans discharged before 1975 who submitted claims to agency might be included
 - **As a result VA had to notify everyone**
- 



What is the issue at UCSF?

- Mobile devices are increasingly being used to store, transmit and receive information at UCSF. **A laptop is stolen at UCSF every week**
- **May 2005 – May 2006** - Approximately 57 Mobile devices (e.g., laptops, memory sticks, PDA's, camera's etc) were reported lost or stolen. 31 of the 57 incidents occurred at the Parnassus campus. Most common ways include;
 - Locked offices
 - Unlocked & unattended offices, labs
 - In vehicles
- **Out of the 57 lost devices, 8 of them required notification. What is notification and why should I care? State Law:** SB-1386 California, Privacy of Personal Information to Prevent Identity Theft. SB 1386 requires mandatory notice to the subject of an unauthorized, unencrypted electronic disclosure of “personal information”. For additional information:
<http://isecurity.ucsf.edu/main.jsp?content=compliance/sb1386>





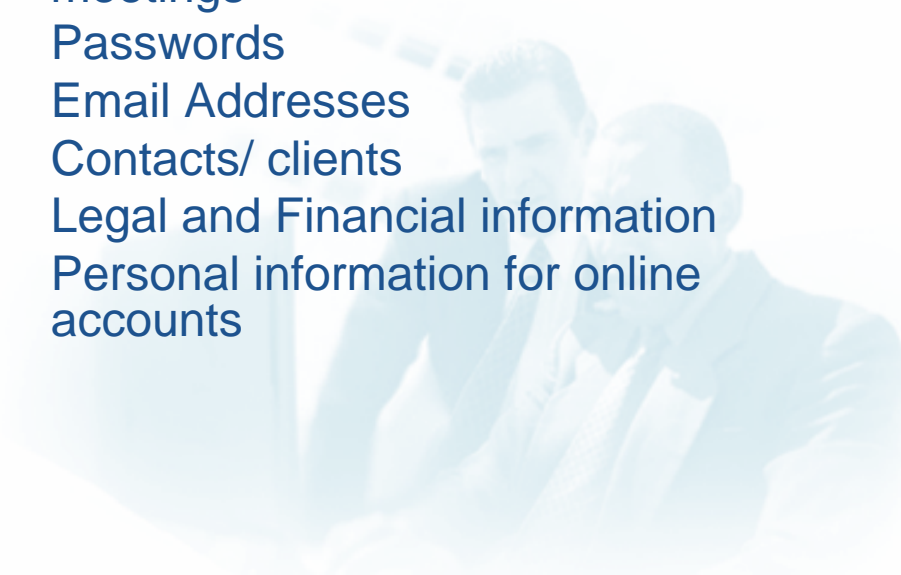
What is at Risk?


What information on mobile devices can be compromised if lost or stolen?



Everything

- UCSF and Your Confidential, Restricted information or Confidential Electronic Information
- Electronic Protected Health Information (EPHI)
- Personally Identified Information (PII)
- Information about appointments/ meetings
- Passwords
- Email Addresses
- Contacts/ clients
- Legal and Financial information
- Personal information for online accounts





What is Confidential Electronic Information?

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



What is “ePHI” and electronic media?

- **ePHI** or electronic Protected Health Information is patient health information which is **computer based**, e.g., created, received, stored or maintained, processed and/or transmitted in electronic media.
- **Electronic media** includes computers, laptops, disks, memory stick, PDAs, servers, networks, dial-modems, E-Mail, web-sites, etc.
- **Reminder** : Federal Laws: HIPAA Privacy & Security Laws mandate protection and safeguards for access, use and disclosure of PHI and/or ePHI with sanctions for violations.





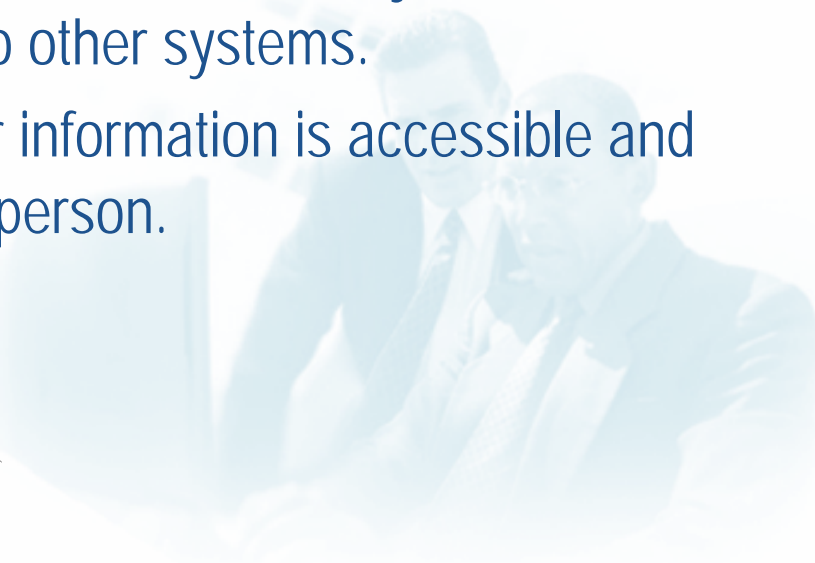
What is “PII”?

- “Personal information” – **Unencrypted computerized information** that includes an individual’s name in combination with any one or more of the following: Social Security Number, Driver’s license number, or California ID card #, credit / debit in combination with their access / security code or password
 - State Law: SB-1386 California, Privacy of Personal Information to Prevent Identity Theft. SB-1386 requires mandatory notice to the subject of an unauthorized, unencrypted electronic disclosure of “personal information”.



What are the Information Security Standards for Protection of ePHI?

- **“Information Security”** means to ensure the confidentiality, integrity, and availability of information through safeguards.
- **“Confidentiality”** – that information will not be disclosed to unauthorized individuals or processes [164.304]
- **“Integrity”** – the condition of data or information that has not been altered or destroyed in an unauthorized manner. Data from one system is consistently and accurately transferred to other systems.
- **“Availability”** – the property that data or information is accessible and useable upon demand by an authorized person.





We all learned the general requirements for protecting information from the **Federal Security Rule (HIPAA)[45 CFR #164.306-a]**



- Ensure the "CIA" (confidentiality, integrity and availability) of all electronic protected health information (ePHI) that the **covered entity** creates, receives, maintains, or transmits.
- Protect against reasonably anticipated threats or hazards to the security or integrity of ePHI, e.g., hackers, virus, data back-ups
- Protect against unauthorized disclosures
- Train workforce members



What are some of the Security Issues with Laptop and other Mobile Device?



- Traveling with your laptop may help you stay connected, but it will also increase your risk of being a target for theft.
- Laptops and mobile devices, being **small**, portable devices, are **easily lost or stolen**. About 250K PDAs were lost in US airports during 2005.(Gartner report)
- Laptops/mobile devices are **frequently used** in hostile environments like hotspots, customer sites, business partner offices, and industry conferences.
- **Attackers are drawn to locations** where business travelers gather, because targets are more plentiful and it is **easier to go unnoticed**.
- Mobile phones can download games, ring tones, and other software have opened a new avenue for hackers to exploit.
- Compact flash/ memory sticks/ PCMCIA cards supported by handhels can store a lot of data on them. These removable cards (and their contents) are easily lost, “borrowed” or stolen.



There are many more risk...



What can you do?





You can help protect UCSF information that you have access to by doing the following:

- Learn and practice “good security computing practices”.
- Incorporate the following 10 **security practices (5 specific to mobile devices and 5 for desktops/workstations)** into your everyday routine. Encourage others to do as well.
- Report anything unusual – Notify the appropriate contacts if you become aware of a suspected security incident.
- If it sets off a warning in your mind, it just may be a problem!



“Good Computing Practices” 10 Safeguards for Users

1. **Workstation Security**
2. **Portable Device Security**
3. **User ID** or Log-In Name (aka. User Access Controls)
4. **Passwords**
5. **Data Management**, e.g., back-up, archive, restore.
6. **Remote Access**
7. **Recycling Electronic Media & Computers**
8. **E-Mail**
9. **Safe Internet Use**
10. **Reporting Security Incidents / Breach**



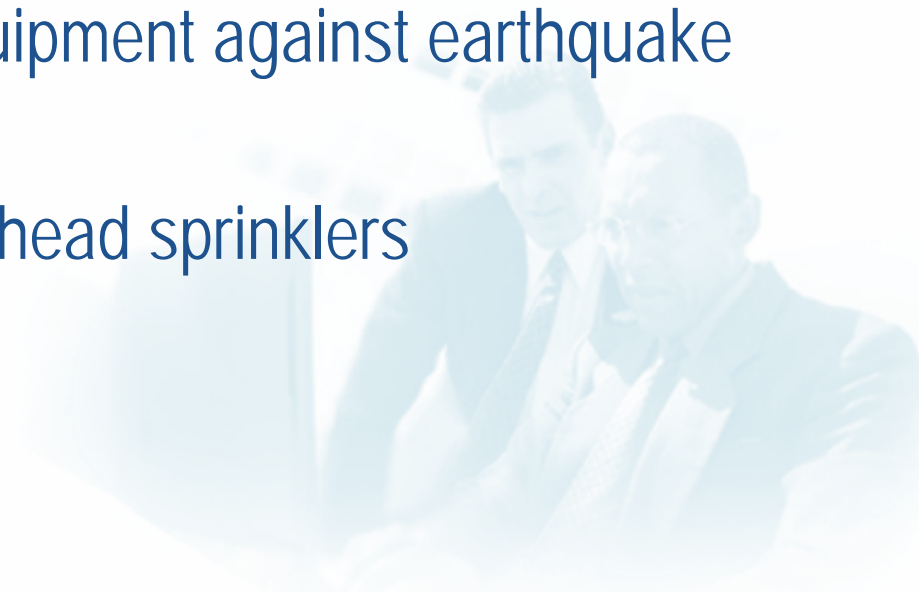
Safeguard-#1: Workstation Security – Physical Security

- **“Workstations”** include any electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.
 - **Physical Security measures include:**
 - Disaster Controls
 - Physical Access Controls
 - Device & Media Controls (*also see Safeguard #4*)
- 




1-1. Workstations: Disaster Controls

- **Disaster Controls:** Protect workstations from natural and environmental hazards, such as heat, liquids, water leaks and flooding, disruption of power, conditions exceeding equipment limits.
- Use electrical surge protectors
- Install fasteners to protect equipment against earthquake damage
- Move servers away from overhead sprinklers



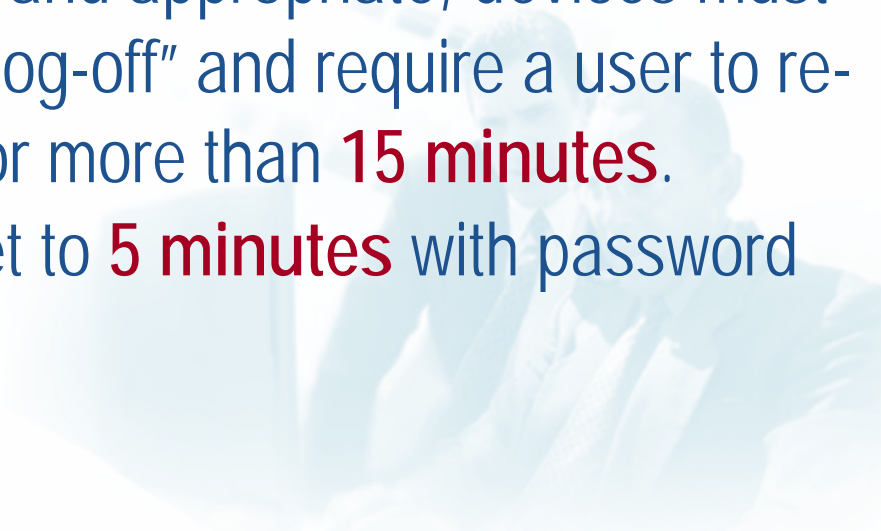


1-2. Workstations: Physical Access Controls

- **Log-off** before leaving a workstation unattended.
 - This will prevent other individuals from accessing EPHI under your User-ID and limit access by unauthorized users.
 - **Lock-up!** – Offices, windows, workstations, sensitive papers and PDAs, laptops, mobile devices / media.
 - Lock your workstation (Cntrl+Alt+Del and Lock) – Windows XP, Windows 2000
 - Encryption tools should be implemented when physical security cannot be provided
 - Maintain key control
 - Do not leave sensitive information on remote printers or copier.
- 



1-3. Workstations: Device Controls

- Unauthorized physical access to an unattended device can result in harmful or fraudulent modification of data, fraudulent email use, or any number of other potentially dangerous situations. These tools are especially important in patient care areas to restrict access to authorized users only.
 - **Auto Log-Off:** Where possible and appropriate, devices must be configured to “lock” or “auto log-off” and require a user to re-authenticate if left unattended for more than **15 minutes**.
 - **Automatic Screen Savers:** Set to **5 minutes** with password protection.
- 



Safeguard-#2: Security for Portable Devices & Laptops with ePHI

- Implement the workstation physical security measures listed in Safeguard #1, including this Check List:
 - Use an Internet Firewall
 - Use **up-to-date** Anti-virus software
 - **Install** computer software **updates**, e.g., Microsoft **patches**
 - **Encrypt** and **password** protect portable devices
 - Lock-it up!, e.g., Lock office or file cabinet, **cable lock**
 - Automatic log-off from programs
 - Use password protected screen savers
 - **Back-up** critical data and software programs

2-1: Security for USB Memory Sticks & Storage Devices

- Memory Sticks are new devices which pack big data in tiny packages, e.g., 256MB, 512MB, 1GB , 4 GB and more.
- Safeguards:
 - Don't store ePHI on memory sticks
 - If you do store it, either de-identify it or use encryption software
 - Delete the ePHI when no longer needed
 - Protect the devices from loss and damage



Delete temporary ePHI files from local drives & portable media too!



2-2. Security for PDAs Personal Digital Assistants

- PDA or Personal Digital Assistants are personal organizer tools, e.g., calendar, address book, phone numbers, productivity tools, and can contain prescribing and patient tracking databases of information and data files with ePHI. PDAs are at risk for loss or theft.
- Safeguards:
 - Don't store ePHI on PDAs
 - If you do store it, de-identify it!; or
 - Encrypt it and password protect it
 - Back up original files
 - Delete ePHI files -- from PDAs, laptops and all portable media when no longer needed
 - Protect it from loss or theft.

Examples: Palm Pilot; HP;
Blackberry; Compaq iPAQ





2-3. Security for Wireless Devices

- Wireless devices open up more avenues for ePHI to be improperly accessed. To minimize the risk, use the following precautions:
 - Do not enable the wireless port that exposes the device, unless it has been secured.
 - Use a Virtual Private Network (VPN), if making a wireless connection
 - Adhere to user / device authentication before transmitting ePHI wirelessly
 - Encrypt data during transmission, and maintain an audit trail.
 - Refer questions to your Information Security Office





Safeguard - #3: Unique User Log-In / User Access Controls

■ Access Controls:

- Users are assigned a unique “User ID” for log-in purposes
- Each individual user’s access to ePHI system(s) is appropriate and authorized
- Access is “role-based”, e.g., **access is limited to the minimum information needed to do your job**
- Unauthorized access to ePHI by former employees is prevented by terminating access
- User access to information systems is logged and audited for inappropriate access or use.



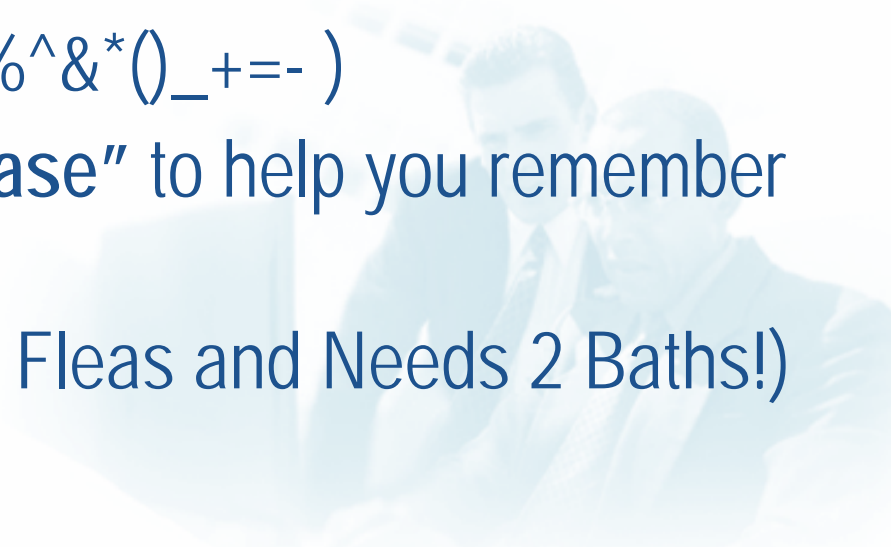
Safeguard-#4: Password Protection

To safeguard YOUR computing accounts, **YOU** need to take steps to protect your password. When choosing a password,

- Don't use a word that can easily be found in a dictionary — English or otherwise.
- Use at least seven characters (letters, numbers, symbols)
- Don't share your password — protect it the same as you would the key to your residence. After all, it is a “key” to your identity.
- Don't let your Web browser remember your passwords. Public or shared computers allow others access to your password.



4-1. Password Construction Standard

- Use seven character minimum and should contain at least one of each of the following characters:
 - Uppercase letters (A-Z)
 - Lowercase letters (a-z)
 - Numbers (0-9)
 - Punctuation marks (!@#\$%^&*()_+ = -)
 - **Better yet, use a “pass-phrase”** to help you remember your password, such as:
 - MdHF&N2B! (My dog Has Fleas and Needs 2 Baths!)
- 



Safeguard-#5: Data Management & Security

Topics in this section cover:

- Data backup and storage
- Transferring and downloading data
- Data disposal





5-1a: Data Backup & Storage

- System back-ups are created to assure integrity and reliability. You can get information about back-up procedures from the Information Administrator for your department. If YOU store original data on local drives or laptops, **YOU are personally responsible** for the data backup and secure storage of data:
- Backup original data files with ePHI and other essential data and software programs frequently based on data criticality, e.g., daily, weekly, monthly.
 - Store back-up disks at a geographically separate and secure location
 - Prepare for disasters by testing the ability to restore data from back-up tapes / disks
- Consider encrypting back-up disks for further protection of confidential information



5-1b. Data Storage - Portable Devices

Also refer to Portable Media Safeguards #4

- Permanent copies of ePHI should not be stored for archival purposes on portable equipment, such as laptop computers, PDAs and memory sticks.
- If necessary, temporary copies could be used on portable computers, only when:
 - The storage is limited to the duration of the necessary use; and
 - If protective measures, such as encryption, are used to safeguard the confidentiality, integrity and availability of the data in the event of theft or loss.



5-2. Transferring & Downloading Data

- Users must ensure that appropriate security measures are implemented before any ePHI data or images are transferred to the destination system.
- Security measures on the destination system must be comparable to the security measures on the originating system or source.
- Encryption is an important tool for protection of ePHI in transit across unsecured networks and communication systems
 - Refer to: UC Policy IS-3, pages 21-22



5-3. Data Disposal Clean Devices before Recycling

- Destroy EPHI data which is no longer needed:
 - “Clean” hard-drives, CDs, zip disks, or back-up tapes before recycling or re-using electronic media
 - Have an IT professional overwrite, **degauss** or destroy your digital media before discarding – via magnets or special software tools; and/or
 - Know where to take these items for appropriate safe disposal



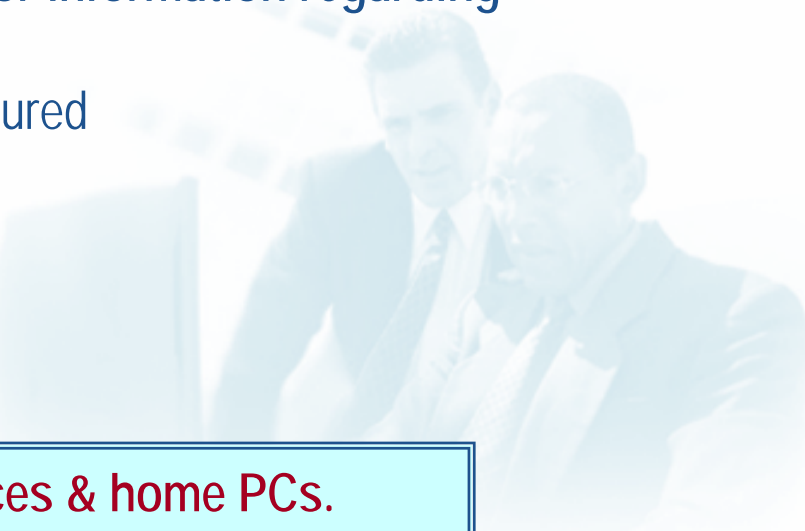
Safeguard-#6: Secure Remote Access

The following minimum standards are required for **remote network access** by portable devices, laptops and home computers connected to the UC network. More stringent standards may apply in individual campus Departments. **Minimum network security standards** are:

1. Software security patch up-to-date
2. Anti-virus software running and up-to-date on every device
3. Turn-off unnecessary services & programs
4. Physical security safeguards to prevent unauthorized access

Contact your Information Security Department for information regarding the following standards:

5. Host-based firewall software – running & configured
6. Minimize unencrypted authentication
7. No unauthenticated email relays to third parties
8. No uncontrolled-access to proxy servers



Apply these same standards to all portable devices & home PCs.



6-1. Virtual Private Network (VPN) for secure remote access to Network with ePHI

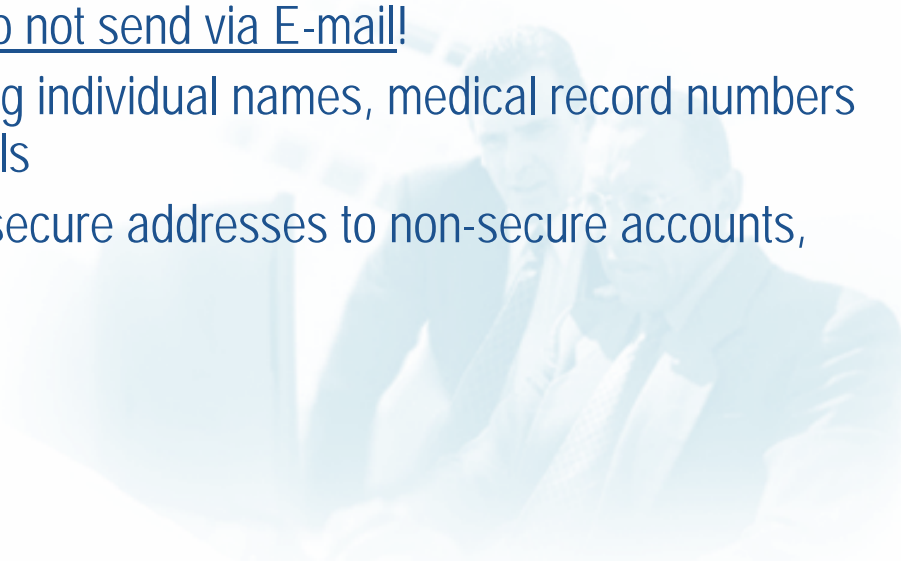
- Rather than receiving ePHI as an E-Mail attachment; or logging in via an unsecure home account, consider using a VPN connection to obtain remote access to ePHI.
- Benefit: A VPN will allow the user to create a secured encrypted link between the user's computer and the UCSF network to view information.
- Contact your computer support resource to determine if this is an option for you. Adhere to the security features of the VPN software.



Safeguard-#7: E-Mail Security

E-mail is like a “postcard”. Email may potentially be viewed in transit by many individuals, since it may pass through several switches enroute to its final destination or never arrive at all! Although the risks to a single piece of email are small given the volume of email traffic, **emails containing ePHI need a higher level of security.**

1. **Use secure, encrypted E-Mail software, if available**
2. **If secure E-Mail is not available, and you need to send an attachment with ePHI: password protect the file or encrypt it or do not send via E-mail!**
3. **Security at the Subject Line:** Avoid using individual names, medical record numbers or account numbers in unencrypted E-Mails
4. **Do not forward E-Mails with ePHI from secure addresses to non-secure accounts, e.g., HotMail, AOL.**





7-1. E-Mail between Patients & Providers

- Use e-mail encryption programs, if available
- If e-mail encryption is not available, obtain consent from patients for use of e-mail which outlines the risks of the e-mail messages
- Review your Medical Center / clinic policies regarding record retention for e-mail messages



7-2. Should You Open the E-mail Attachment?



- **If it's suspicious, don't open it!**
- What is suspicious?
 - Not work-related
 - Attachments not expected
 - Attachments with a suspicious file extension (*.exe, *.vbs, *.bin, *.com, *.scr, or *.pif)
 - Web link
 - Unusual topic lines; "Your car?"; "Oh!"; "Nice Pic!"; "Family Update!"; "Very Funny!"





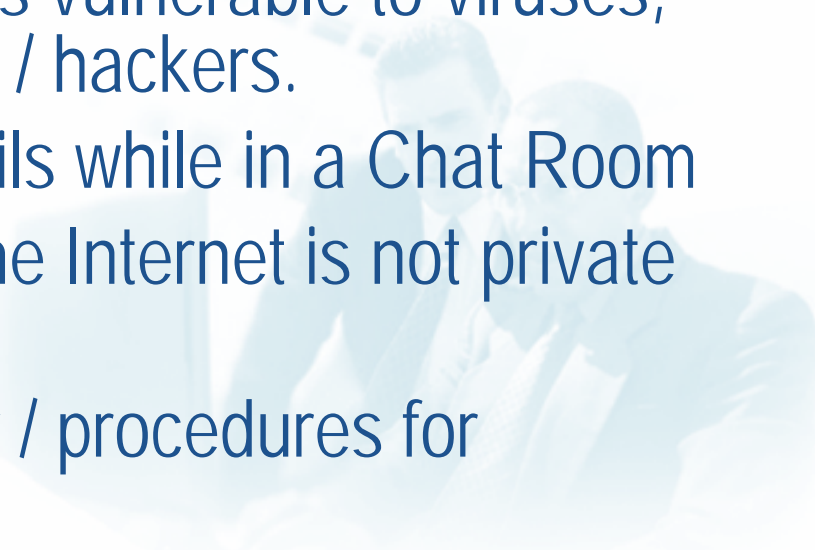
7-3. E-Mail Security – Risk Areas

- 1. Spamming.** Unsolicited bulk e-mail, including commercial solicitations, advertisements, chain letters, pyramid schemes, and fraudulent offers.
 - Do not reply to spam messages. Do not spread spam. Remember, sending chain letters is against UC policy.
 - Do not forward chain letters. It's the same as spamming!
 - Do not open or reply to suspicious e-mails.
- 2. Phishing Scams.** E-Mail pretending to be from trusted names, such as Citibank or Paypal or Amazon, but directing recipients to rogue sites. A reputable company will never ask you to send your password through e-mail.
- 3. Spyware.** Spyware is adware which can slow computer processing down; hijack web browsers; spy on key strokes and cripple computers



7-4. Instant Messaging (IM) - Risks

- Instant messaging (IM) and Instant Relay Chat (IRC) or chat rooms create ways to communicate or chat in “real-time” over the Internet.
- Exercise caution when using Instant Messaging on UC Computers:
 - Maintain up-to-date virus protection and firewalls, since IM may leave networks vulnerable to viruses, spam and open to attackers / hackers.
 - Do not reveal personal details while in a Chat Room
 - Be aware that this area of the Internet is not private and subject to scrutiny
 - Refer to your campus policy / procedures for guidance



Safeguard-#8: Internet Use



- UC encourages the use of Internet services to advance the University's mission of education, research, patient care, and public service.
- UC's Electronic Communications Policy governs use of its computing resources, web-sites, and networks.
 - Appropriate use of UC's electronic resources must be in accordance with the University principles of academic freedom and privacy.
- Protection of UC's electronic resources requires that everyone use responsible practices when accessing online resources.
 - Be suspicious of accessing sites offering questionable content. These often result in spam or the release of viruses.
- Be careful about providing personal, sensitive or confidential information to an Internet site or to web-based surveys that are not from trusted sources.
- <http://www.ucop.edu/ucophome/policies/ec/brochure.pdf>

Remember: **The Internet is not private!** Access to any site on the Internet could be traced to your name and location.




8-1. Internet Use: Privacy Cautions

- Personal information posted to web-pages may not be protected from unauthorized use.
- Even unlinked web pages can be found by search engines
- Some web sites try to place small files ("cookies") on your computer that might help others track the web pages you access
- Web sites on UC servers should tell users how to contact the owner or webmaster
- Campus policies must determine access rights for 3rd parties or outside organizations. In some cases, a HIPAA Business Associate Agreement may be also required.



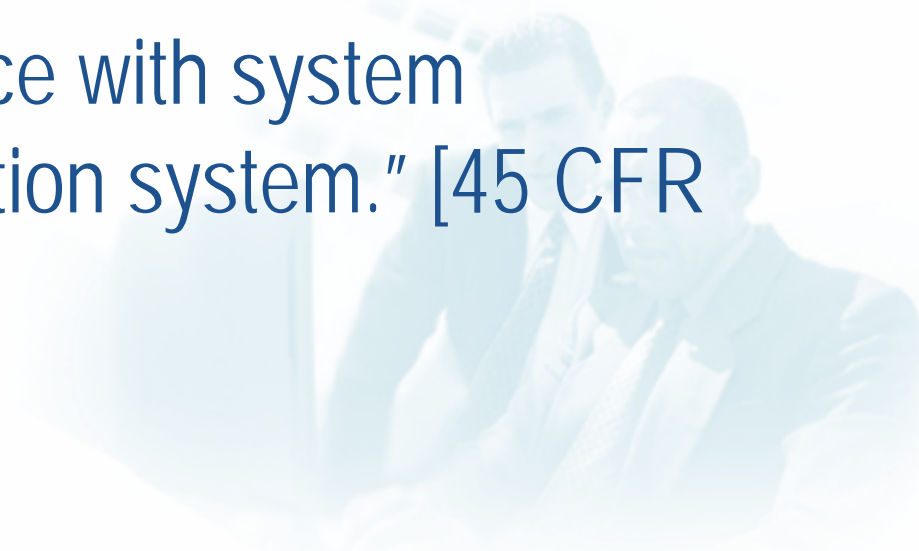
Safeguard-#9: Report Security Incidents

- You are responsible to:
 - Report and respond to security incidents and security breaches.
 - Know what to do in the event of a security breach or incident related to ePHI and/or Personal Information.
 - Report security incidents & breaches to:
 - ITS Customer Support 415-514-1400 (option 2)
 - Email: itscs@its.ucsf.edu
- 



9-1. Security Incidents and ePHI (HIPAA Security Rule)

- Security Incident defined:
- “The attempted or successful or improper instance of unauthorized access to, or use of information, or mis-use of information, disclosure, modification, or destruction of information or interference with system operations in an information system.” [45 CFR 164.304]





9-2. Security Breach and Personal Information (SB-1386, Protection of Personal Information Law)

- **“Security breach”** per UC Information Security policy (IS-3) is when a California resident’s **unencrypted** personal information is reasonably believed to have been acquired by an unauthorized person. **PII means:**
 - Name + SSN + Drivers License +
 - Financial Account /Credit Card Information
- Good faith acquisition of personal information by a University employee or agent for University purposes does not constitute a security breach, provided the personal information is not used or subject to further unauthorized disclosure.



Safeguard-#10: Your Responsibility to Adhere to UC-Information Security Policies

- Users of electronic information resources are responsible for familiarizing themselves with and complying with all University policies, procedures and standards relating to information security.
- Users are responsible for appropriate handling of electronic information resources (e.g., ePHI data)
 - Reference: UC Policy #IS-3, Campus Policy and campus "Computer Security & Use Agreement"






10-1. Safeguards: Your Responsibility

- Protect your computer systems from unauthorized use and damage by using:
 - Common sense
 - Simple rules
 - Technology
- **Remember** – By protecting yourself, you're also doing your part to protect UCSF and our patient and employee confidential data and information systems.



Security Reminders

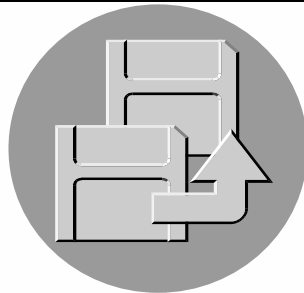


Password
Required

Password protect
your computer



Keep office secured



Backup your electronic
information



Keep disks
locked up



Run Anti-virus &
Anti-spam software,
Anti-spyware



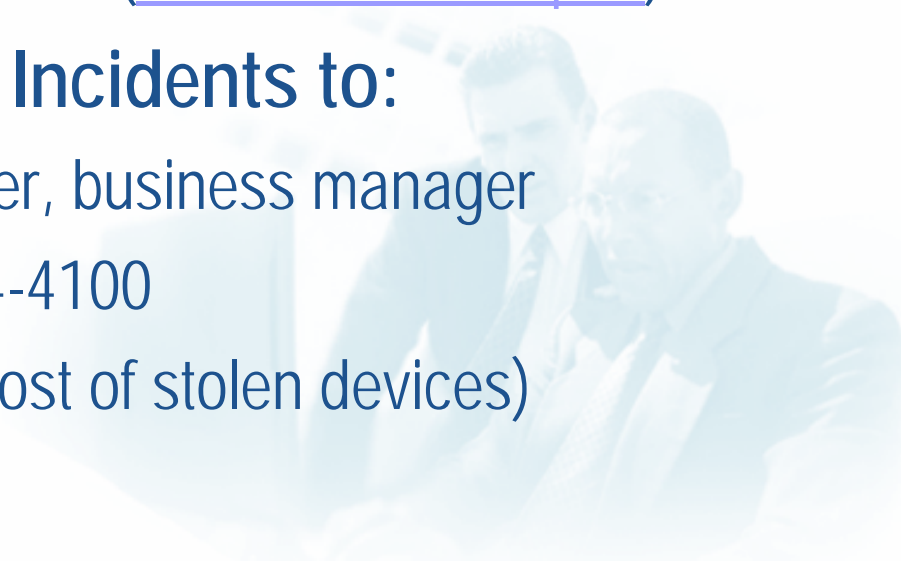
10-2. Sanctions for Violators

- Workforce members who violate UC policies regarding privacy / security of confidential, restricted and/or protected health information or ePHI are subject to further corrective and disciplinary actions according to existing policies.
- Actions taken could include:
 - Termination of employment
 - Possible further legal action
 - Violation of local, State and Federal laws may carry additional consequences of prosecution under the law, costs of litigation, payment of damages, (or both); or all.
 - Knowing, malicious intent → Penalties, fines, jail!



Resources for Reporting Security Incidents

- Your Department's IT Resource or Support person
- UCSF security incident contacts:
 - UCSF ITS Customer Support: 415-514-4100
 - UCSF HIPAA Security Procedures, Electronic Security Policies and the HIPAA Handbook (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)





UCSF Is Only as Strong As Our Weakest Link.

Help UCSF maintain a strong defense
and secure our confidential information



Resources and References

- Talk to your departmental manager
- UCSF Information Security Officer (ctianen@its.ucsf.edu)
- UCSF HIPAA Security Procedures, Electronic Security Policies and the HIPAA Handbook (www.ucsf.edu/hipaa)
- UC Information Security Policy
<http://www.ucop.edu/ucophome/policies/bfb/is3.pdf>
- Report Suspected Security Incidents to:
 - **Dept CSC**
 - **IT Customer Support: 514-4100**
 - **UCSF Police: 476-1414**
- For additional information about other security awareness materials, go to <http://isecurity.ucsf.edu>



***Thank you
for helping UCSF protect the security
of our patients'
Confidential Information. You have
completed the Basic Component of
the
Security Awareness Training.***

