



Information Security Awareness Training: “Good Computing Practices” for Confidential Electronic Information

For All HIPAA Workforce Members
Revised April 2013

This presentation focuses on two types of restricted electronic information:

- ▶ **ePHI = Electronic Protected Health Information**

- Medical record number, account number or SSN
- Patient demographic data, e.g., address, date of birth, date of death, sex, e-mail / web address
- Dates of service, e.g., date of admission, discharge
- Medical records, reports, test results, appointment dates

- ▶ **PII = Personally Identified Information**

- Individual's name + SSN number + Driver's License # & financial credit card account numbers
- Medical history, mental or physical condition, or medical treatment
- Health insurance policy #, subscriber ID#, application & claims history/appeals records

Definition of “ePHI”

- ▶ **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, CDs/DVDs/disks, memory sticks, smart phones, PDAs, servers, networks, dial-modems, email, web-sites, etc.

Federal Laws: HIPAA Privacy & Security Laws mandate protection and safeguards for access, use and disclosure of PHI and/or ePHI with sanctions for violations.

Definition of “PII”

- ▶ Personal identity information (PII) is the electronic manifestation of an individual’s first name or first initial, and last name, in combination with one or more of the following:
 - Social Security number, Drivers license #, State-issued ID Card #, Account #, credit or debit card # in combination with any required security code, access code, or password that could permit access to an individual’s financial account
 - Medical information, history, mental or physical condition, treatment or diagnosis by a health care professional
 - Health insurance information, policy # or subscriber ID #, unique identifier, any information in an application & claims history, including any appeals records

The definition of electronic PII is not dependent on where the personal identity information is stored.

State Law: California Civil Code 1798.29 of the California Information Practices Act 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?

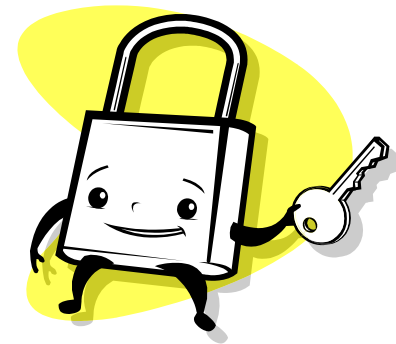


- ▶ **“Information Security”** means to ensure the confidentiality, integrity, and availability of information through safeguards.
- ▶ **“Confidentiality”** – that information will not be disclosed to unauthorized individuals or processes [164.304]
- ▶ **“Integrity”** – the condition of data or information 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 data or information is accessible and useable upon demand by an authorized person.

What are the Federal Security Rule

General Requirements? [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 (“awareness of good computing practices”)



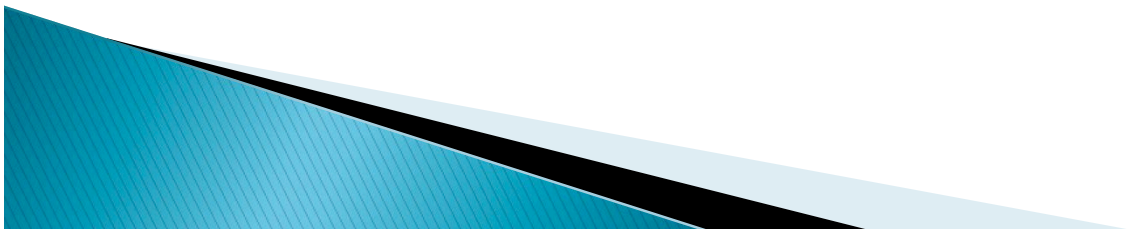
Compliance required since April 20, 2005

Why do I need to learn about Security – *“Isn’t this just an IT Problem?”*

Good Security Standards follow the “90 / 10” Rule:

- ▶ 10% of security safeguards are technical
- ▶ 90% of security safeguards rely on the computer user (“YOU”) to adhere to good computing practices

Example: The lock on the door is the 10%. You remembering to lock, check to see if it is closed, ensuring others do not prop the door open, keeping controls of keys is the 90%. 10% security is worthless without YOU!

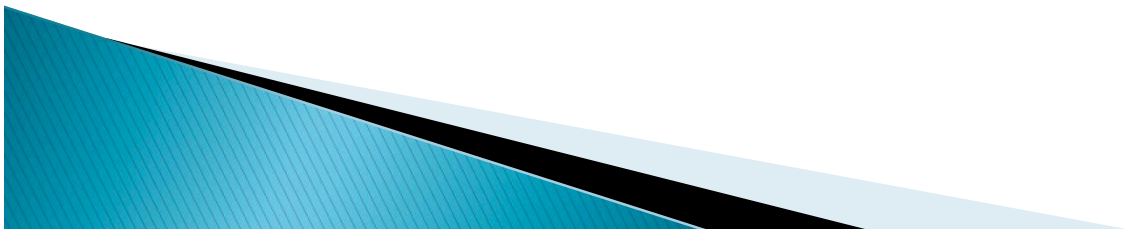


What are the Consequences for Security Violations?

- ▶ Risk to integrity of confidential information, e.g., data corruption, destruction, unavailability of patient information in an emergency
- ▶ Risk to security of personal information, e.g., identity theft
- ▶ Loss of valuable business information
- ▶ Loss of confidentiality, integrity & availability of data (and time) due to poor or untested disaster data recovery plan
- ▶ Embarrassment, bad publicity, media coverage, news reports
- ▶ Loss of patients' trust, employee trust and public trust
- ▶ Costly reporting requirements for breaches under CA Civil Code
- ▶ Internal disciplinary action(s), termination of employment
- ▶ Penalties, prosecution and potential for sanctions / lawsuits

Security Objectives

- ▶ Learn and practice “good computer security practices” .
- ▶ Incorporate the following **10 security practices** 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. Unique User ID or Log-In Name (aka. User Access Controls)
2. Password Protection
3. Workstation Security – Physical Security
4. Security for Workstations, Portable Devices & Laptops with ePHI
5. Data Management, e.g., back-up, archive, restore, disposal.
6. Secure Remote Access
7. E-Mail Security
8. Safe Internet Use
9. Reporting Security Incidents / Breaches
10. Your Responsibility to Adhere to UC Information Security Policies

Safeguard #1

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 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 #2

Password Protection

Passwords that provide access to ePHI **must comply with UCSC's Password Standards** (<http://its.ucsc.edu/policies/password.html>):

- ▶ **Use at least 8 characters and include at least 3 of the 4 following types of characters:**
 - Uppercase & Lowercase letters (A-Z , a-z)
 - Numbers (0-9)
 - Special characters
 - Punctuation marks (!@#\$%^&*()_+ = -)
- ▶ **Try a “passphrase”** to help you remember your password, e.g.:
 - MdHF&NAW! (My dog Has Fleas and Needs A Wash!)
 - Buffalo Space Radar! (random but memorable strings of words)

#2-1. Password Protection (cont.)

Additional guidance for password security:

- ▶ Longer passwords are better.
- ▶ Don't use a dictionary word, forward or backward – in any language – or a word preceded or followed by a single number (e.g. Password1).
- ▶ Don't use your user name or login name as a password.
- ▶ Don't use a common keyboard sequence, such as "qwerty89" or "abc123".
- ▶ Don't share or reveal your password, including to co-workers, your supervisor, or IT staff. Your password is your personal signature. No one else should know it or ask for it.
- ▶ Don't let your Web browser or applications remember your passwords.

Safeguard #3

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*)

#3-1. 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



#3-2. 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, smart phones, PDAs, laptops, mobile devices / media.
 - Lock your workstation
 - Lock up portable devices or take them with you
 - Encryption tools should be implemented when physical security cannot be provided
 - Maintain key control
 - Do not leave sensitive information on printers or copiers

#3-3. 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:** Devices must be configured to “lock” or “auto log-off” and require a user to re-authenticate if left unattended for more than **10 minutes**.
- ▶ **Automatic Screen Savers:** Set to **10 minutes** with password protection.

Safeguard #4

Security: Workstations, Portable Devices & Laptops that store or access ePHI

- ▶ **Implement the workstation physical security measures listed in Safeguard #3, including this Check List:**
 - Use a Firewall; default settings are typically fine
 - 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
 - Automatic log-off or lock when inactive
 - Use password protected screen savers
 - Back up critical data and software programs
 - Securely delete ePHI and PII when it is no longer needed

#4-1. Security for Portable Devices and Media

- ▶ Portable devices such as smart phones and PDAs can be used for many of the same functions as a standard computer. Any sensitive information they contain must be protected. These devices are also at greater risk for loss or theft than larger devices.
- ▶ Memory Sticks and external hard drives pack big data in tiny packages.
- ▶ **Safeguards:**
 - Don't store ePHI or PII on portable devices, memory sticks or other portable media, including external hard drives
 - If you do store it, de-identify it or encrypt it
 - Password protect portable devices
 - Securely delete ePHI and PII when no longer needed
 - Back up original files
 - Protect these devices from theft and loss – lock them up or keep them with you at all times.



#4-2. Wireless Security

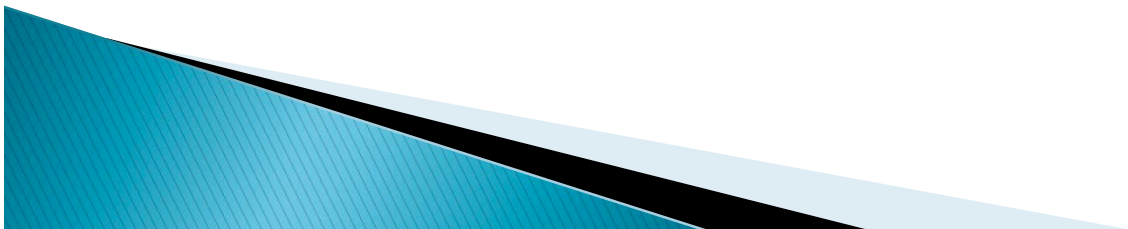
- ▶ **Wireless opens up more avenues for data to be improperly accessed. To minimize the risk, make sure you have a secure (encrypted) connection before working with sensitive data.**
 - Use known, encrypted networks, such as a Virtual Private Network (VPN) or UCSC's EDUROAM SECURE WIRELESS, available to UCSC students, researchers, faculty, and staff (<http://its.ucsc.edu/wireless-secure/>).
 - Make sure web pages have **https** (not **http**) in the web address (URL). The "s" stands for "secure" and tells you that the information you enter is being encrypted as it is sent. Look for this before logging into anything.
 - Coffee shop/hotel/airport-type wireless is not encrypted.
 - Don't connect to unknown wireless hot spots/access points.
If you're not sure, assume it's not secure.

Safeguard #5

Data Management & Security

Topics in this section cover:

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



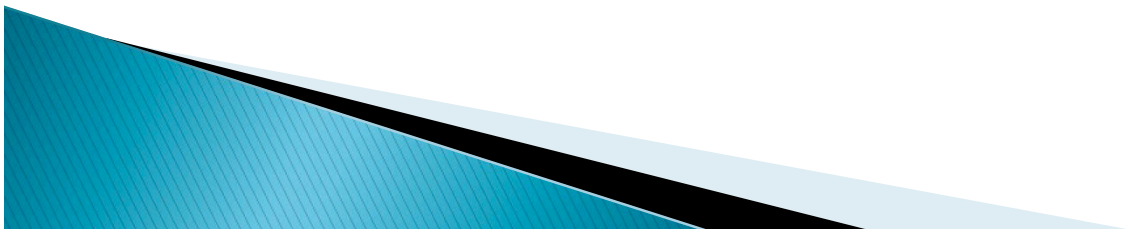
#5-1a. Data Backup & Storage

- ▶ 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 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

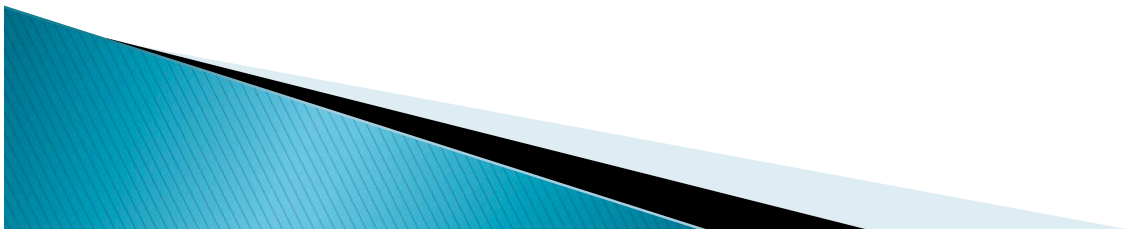
Also refer to [Portable Media Safeguards #4](#)

- ▶ **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 may 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 a system.
- ▶ Security measures on the destination system must be comparable to the security measures on the originating system or source.
- ▶ Encryption is required for protection of ePHI in transit across unsecured networks and communication systems
 - Refer to: UC Policy IS-3, section titled “Encryption”



#5-3. Data Disposal

Clean Devices before Recycling

- ▶ **Destroy ePHI and PII 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.

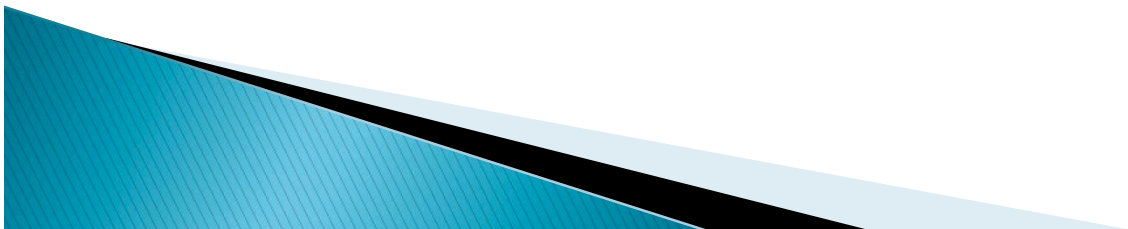


Safeguard #6

Secure Remote Access

All remote access of ePHI and PII – data and systems – must be encrypted.

- ▶ This can be accomplished by using a VPN or other secure connection methods. Consult with ITS for assistance if needed.
- ▶ Remote access to a HIPAA workstation requires departmental approval.



Safeguard #7

Email Security

Email is like a “postcard”.

Email may potentially be viewed in transit by many individuals, since it may pass through several systems 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.**

PLEASE NOTE: For people taking both this training and UC’s HIPAA Training at learningcenter.ucsc.edu:

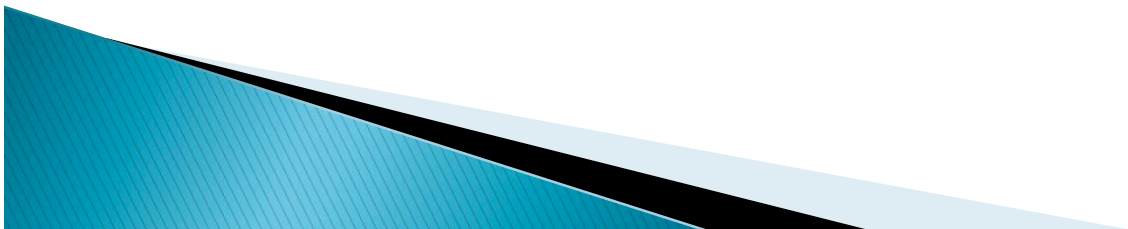
This section presents UCSC-specific requirements for the use of email with ePHI and PII. The requirements in this section **supersede** the information in UC’s HIPAA Training at learningcenter.ucsc.edu.

#7-1. Emailing ePHI and PII

Email is not a secure method for transmitting restricted data such as ePHI and PII. Only the Benefits Office is allowed to email ePHI and only via encrypted attachment.

- ▶ Student Health Services is to use its secure messaging tool instead of email for communicating about ePHI with patients.

PII must be encrypted if sent via email or other insecure method.



#7-2. Email Security – Risk Areas

1. **Phishing Scams.** Email pretending to be from trusted organizations, such as Citibank, PayPal, Amazon, or even UCSC, asking for your password or other private information. A reputable company will never ask you to send your password through email.
2. **“Click this link” or “open this attachment” scams.** Also a type of phishing, these emails try to trick you into opening a harmful attachment or clicking on a link that directs you to rogue sites or compromises your computer.
3. **Spamming.** Unsolicited bulk email, including commercial solicitations, advertisements, chain letters, pyramid schemes, and fraudulent offers.
 - Do not reply to spam messages. Do not spread or forward spam.
 - Do not open or reply to suspicious emails.

#7-3. Should You Open that Attachment?

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

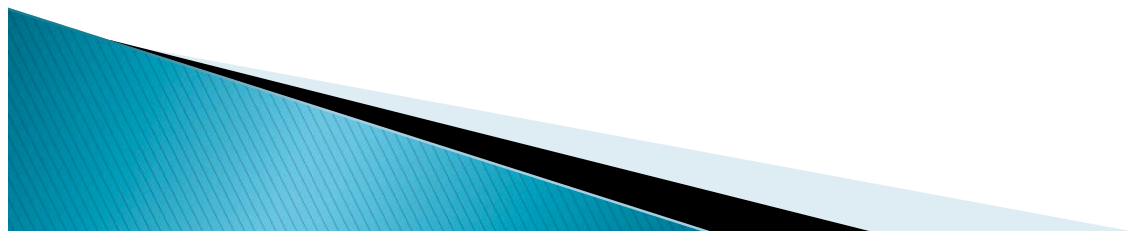


#7-4. ePHI Email Storage

- Long term storage of ePHI on email servers is not allowed under UCSC's HIPAA Security Rule Policy (<http://policy.ucsc.edu/html/it0001.html>).
- The following steps outline proper handling of ePHI in email:
 1. ePHI email(s) must be deleted immediately after sending or receiving.
 2. Delete your email trash at the end of each session
 - For web mail, select the email in your Trash folder and click “delete forever” at the top of the folder).
 - If you are using an email client (Thunderbird, Apple Mail, Outlook, etc.) instead of the gmail web client, you also need to “compact mailboxes” to make sure the email is really gone.
 - See IT Request Knowledge Base article #16804 for instructions: https://ucsc.service-now.com/kb_view.do?sysparm_article=KB0016804

#7-4. ePHI Email Storage continued

Any emails containing ePHI data that may need to be stored for legitimate business or retention purposes must be downloaded to a secure, HIPAA compliant location, then deleted from email according to the instructions on the previous slide.



#7-5. Instant Messaging (IM) - Risks

- ▶ **Texting, instant messaging (IM) and Instant Relay Chat (IRC) or chat rooms create ways to communicate or chat in “real-time” over the Internet.**

- ▶ **Exercise extreme caution when using Instant Messaging on devices that store or access sensitive data or systems:**
 - Maintain up-to-date virus protection and firewalls, since IM may leave devices vulnerable to viruses, spam and open to attackers / hackers.
 - Do not reveal personal details while texting/chatting
 - Be aware that this method of communication is not private and is subject to eavesdropping/snooping.

Safeguard #8:

Internet Use



- ▶ UC's Electronic Communications Policy governs use of its computing resources, web-sites, and networks.
 - 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 from unknown links, or sites offering questionable content. These can result in information theft, viruses or spam.
- ▶ **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.

Safeguard #9:

Security Incidents and ePHI (HIPAA Security Rule)

- ▶ **Security Incident defined**

“The attempted or successful 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]

#9-1. Security Breach and Personal Information (CA Civil Code, Information Practices Act)

- ▶ “**Security breach**” per CA Civil Code and 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, or State ID Card#, or
 - Financial Account /Credit Card Information
 - Specific Medical or Health Insurance 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.

#9-2. 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.
- ▶ SHS employees report security incidents & breaches to:
 - Business Manager or Medical Records Administrator verbally and in writing on the Health Center Incident Report
- ▶ All other employees report to a manager or supervisor. Managers and supervisors report to:
 - ITS Support Center: 459-HELP (4357), 54 Kerr Hall, help@ucsc.edu, or itrequest.ucsc.edu
 - Also cc security@ucsc.edu

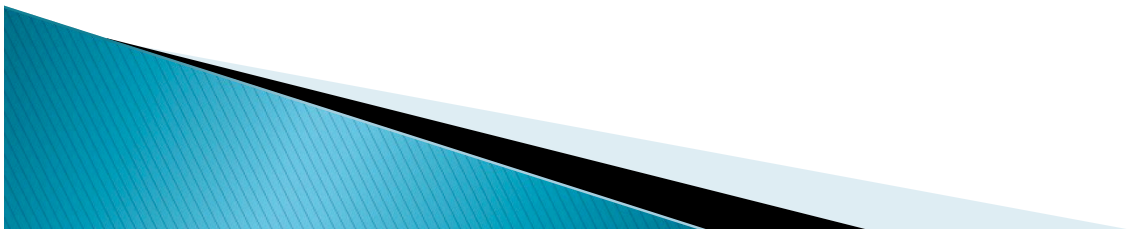
Safeguard #10:

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 and PII data)
 - Reference: <http://its.ucsc.edu/policies/>
 - ✓ UC Information Security Policy IS-3
 - ✓ UC Electronic Communications Policy
 - ✓ Campus HIPAA Policy and Practices for Compliance
 - ✓ Other campus IT Policies

#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 UC and our patient and employee confidential data and information systems.



#10-2. Security Reminders

- ✓ Choose good passwords and keep them secret and secure
- ✓ Password protect your computer and portable devices
- ✓ Set devices to automatically lock after no more than 10 min of inactivity
- ✓ Keep your operating system and applications patched and up to date
- ✓ Run anti-virus & anti-malware software, and keep it up to date
- ✓ Back up critical electronic information
- ✓ Securely delete ePHI and PII when it is no longer needed
- ✓ Log out and lock up/put things away before leaving an area unattended; keep portable devices and media locked up or with you
- ✓ Turn on your device's firewall
- ✓ Encrypt any ePHI or PII stored on portable devices or media
- ✓ Be aware of and report suspected security incidents

#10-3. Sanctions for Violators

- ▶ Workforce members who violate UC policies regarding privacy / security of confidential, restricted and/or protected health information, including ePHI, are subject to corrective and disciplinary actions according to existing University policies.
- ▶ **Actions taken could include:**
 - Termination of employment
 - 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!

Campus Resources for Reporting Security Incidents

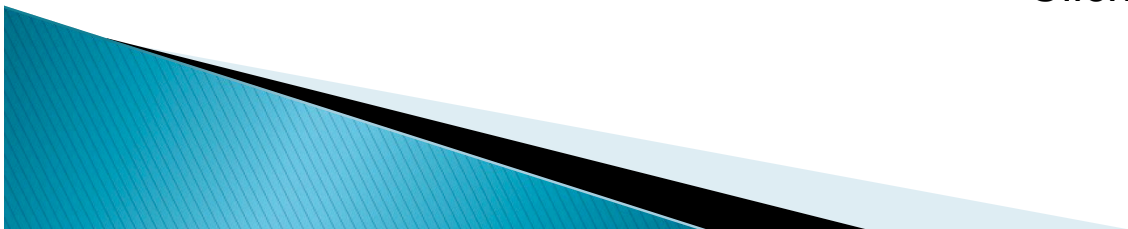
- ▶ For Student Health Services Employees:
 - Robert Antonino - 459-5623
Information Systems Coordinator
 - Cathy Sanders – 459-1628
Medical Records and System Administrator

- ▶ For Everyone:
 - ITS Support Center itrequest.ucsc.edu, 459-HELP (4357), help@ucsc.edu, or 54 Kerr Hall
 - please cc security@ucsc.edu

Quiz Time!

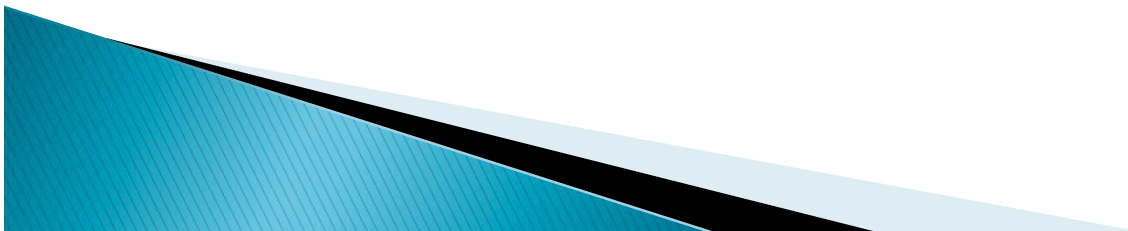
1. ePHI is an acronym for?
 - a. Electronic Personal Health Information
 - b. Electronic Protected Health Information
 - c. Electronic Private Health Information
 - d. Electronic Protected Hospital Information

Click the next slide for the correct answer



Quiz Time!

1. ePHI is an acronym for?
 - a. Electronic Personal Health Information
 - b. Electronic Protected Health Information**
 - c. Electronic Private Health Information
 - d. Electronic Protected Hospital Information

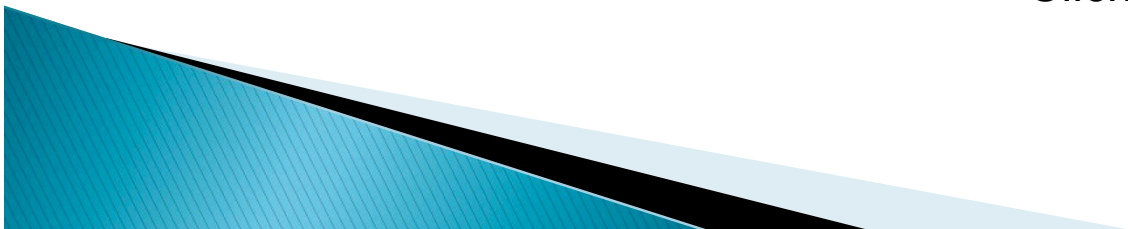


Quiz Time!

2. You only need to protect health information if it is electronic. HIPAA does not require paper-based health information to be protected.

- True
- False

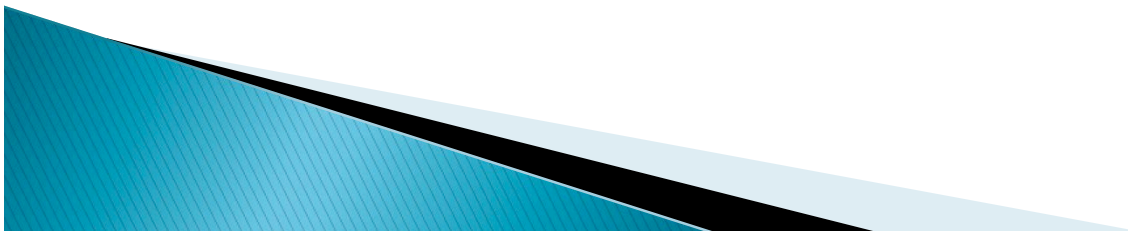
Click the next slide for the correct answer



Quiz Time!

2. You only need to protect health information if it is electronic. HIPAA does not require paper-based health information to be protected.

- True
- **False**




Quiz Time!

3. Personal identity information (PII) is a person's first name or first initial, and last name, in combination with
(Choose all that apply):
- a. Social Security Number (SSN) or financial account numbers
 - b. Home address or home telephone number
 - c. Medical or health insurance information
 - d. Ethnicity or gender



Click the next slide for the correct answer

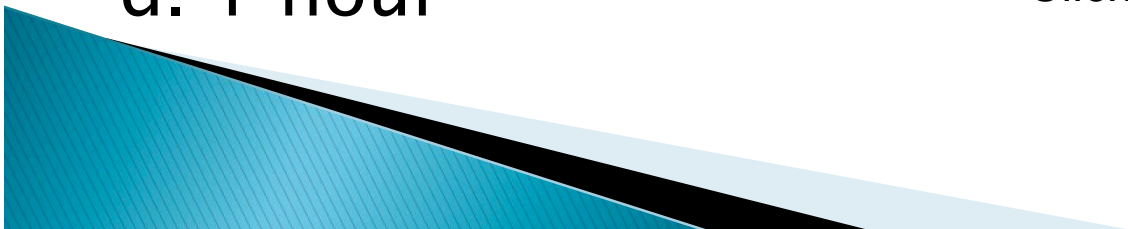
Quiz Time!

3. Personal identity information (PII) is a person's first name or first initial, and last name, in combination with
(Choose all that apply):
- a. **Social Security Number (SSN) or financial account numbers**
 - b. Home address or home telephone number
 - c. **Medical or health insurance information**
 - d. Ethnicity or gender
- 

Quiz Time!

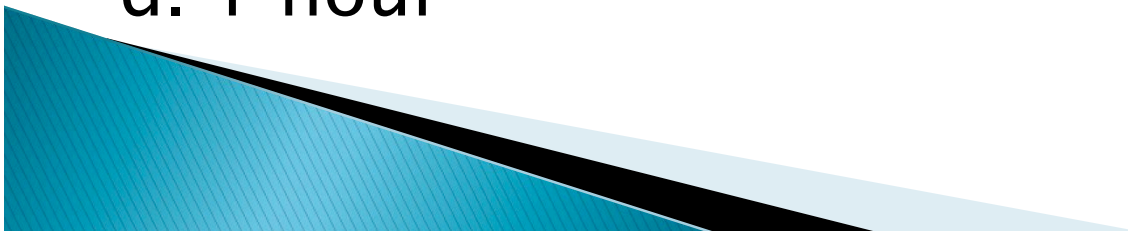
4. Where possible and appropriate, devices that store or access ePHI must be configured to “lock” or “auto log-off” and require a user to re-authenticate if left unattended for more than:
- a. 10 minutes
 - b. 20 minutes
 - c. 30 minutes
 - d. 1 hour

Click the next slide for the correct answer



Quiz Time!

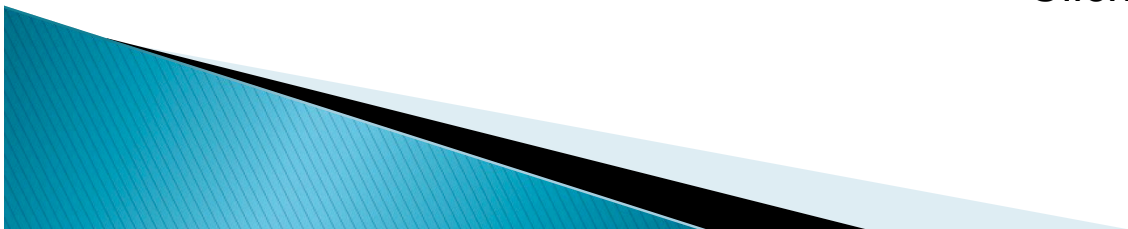
4. Where possible and appropriate, devices that store or access ePHI must be configured to “lock” or “auto log-off” and require a user to re-authenticate if left unattended for more than:
- a. **10 minutes**
 - b. 20 minutes
 - c. 30 minutes
 - d. 1 hour



Quiz Time!

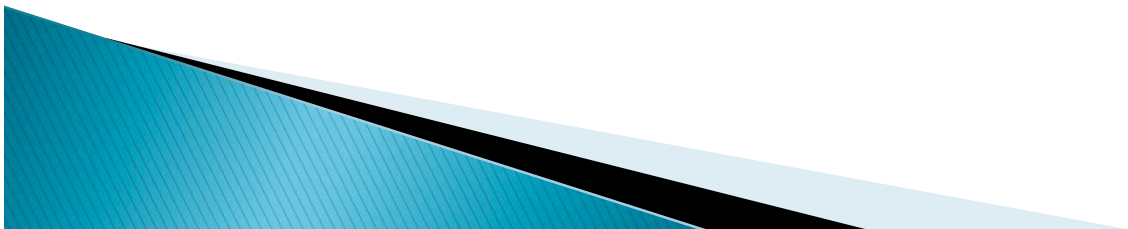
5. Do not access ePHI over a wireless connection unless you are using a(n):
- a. Private wireless router
 - b. Approved University computer
 - c. Strong password
 - d. Encrypted connection

Click the next slide for the correct answer



Quiz Time!

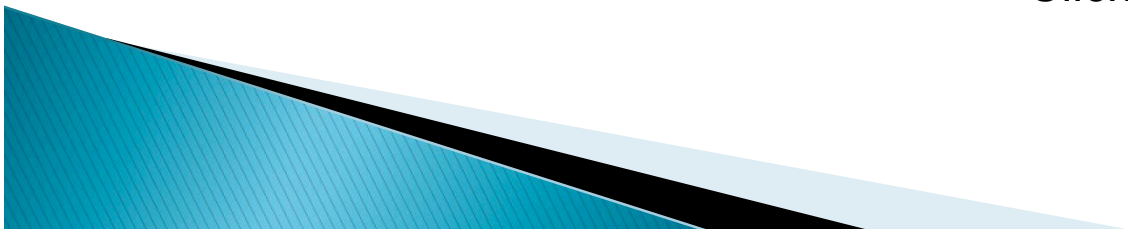
5. Do not access ePHI over a wireless connection unless you are using a(n):
- a. Private wireless router
 - b. Approved University computer
 - c. Strong password
 - d. Encrypted connection**



Quiz Time!

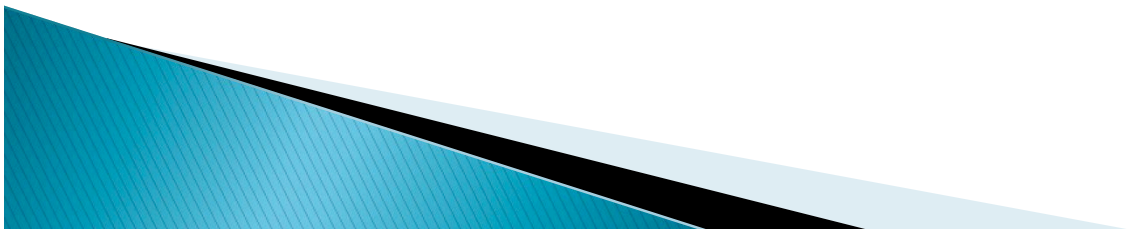
6. Email containing ePHI must be:
- a. Stored on the email server so it's safe
 - b. Stored in your email in case you need it later
 - c. Deleted immediately after you send or receive them
 - d. Deleted from your inbox and "sent" folder, but it's OK to leave a copy in the trash

Click the next slide for the correct answer



Quiz Time!

6. Email containing ePHI must be:
- a. Stored on the email server so it's safe
 - b. Stored in your email in case you need it later
 - c. Deleted immediately after you send or receive them**
 - d. Deleted from your inbox and "sent" folder, but it's OK to leave a copy in the trash



Quiz Time!

7. If you work with ePHI, which of the following storage safeguards are required (choose all that apply):
- a. Store the least amount of ePHI possible
 - b. Destroy ePHI when you are done with it
 - c. Keep backup copies of ePHI near your computer at all times, just in case
 - d. Do not use portable devices for long term ePHI storage

Click the next slide for the correct answer



Quiz Time!

7. If you work with ePHI, which of the following storage safeguards are required (choose all that apply):
- a. **Store the least amount of ePHI possible**
 - b. **Destroy ePHI when you are done with it**
 - c. Keep backup copies of ePHI near your computer at all times, just in case
 - d. **Do not use portable devices for long term ePHI storage**



Quiz Time!

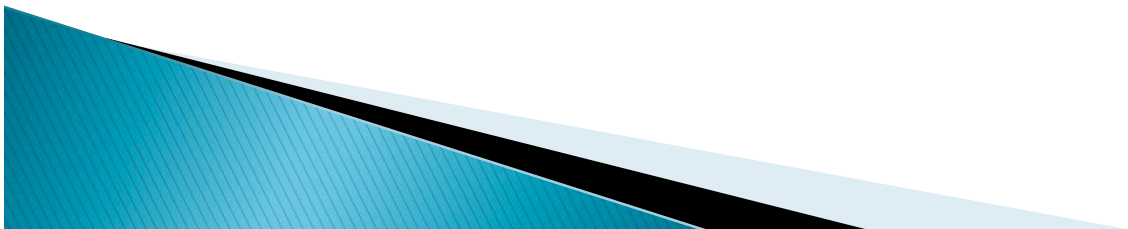
8. Users of electronic information resources are responsible for:
- a. Complying with UC and UCSC policies, procedures and standards
 - b. Appropriate handling of resources
 - c. Reporting suspected security incidents
 - d. All of the above
 - e. None of the above

Click the next slide for the correct answer



Quiz Time!

8. Users of electronic information resources are responsible for:
- a. Complying with UC and UCSC policies, procedures and standards
 - b. Appropriate handling of resources
 - c. Reporting suspected security incidents
 - d. All of the above**
 - e. None of the above

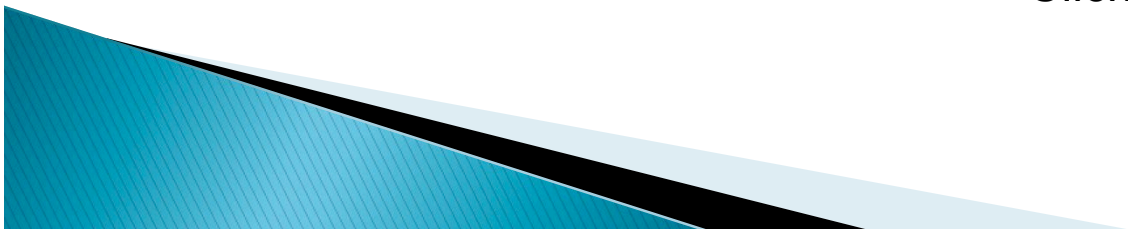


Quiz Time!

9. Only supervisors are responsible for knowing what to do in the case of a security incident or security breach.

- True
- False

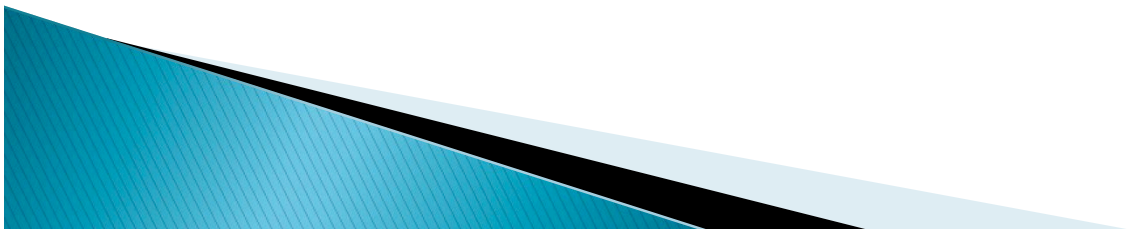
Click the next slide for the correct answer



Quiz Time!

9. Only supervisors are responsible for knowing what to do in the case of a security incident or security breach.

- True
- **False**

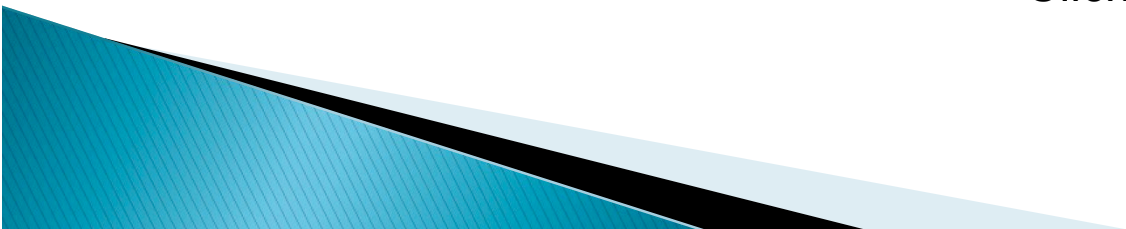


Quiz Time!

10. It's OK to use someone else's password to access ePHI if you are both authorized for the same access.

- True
- False

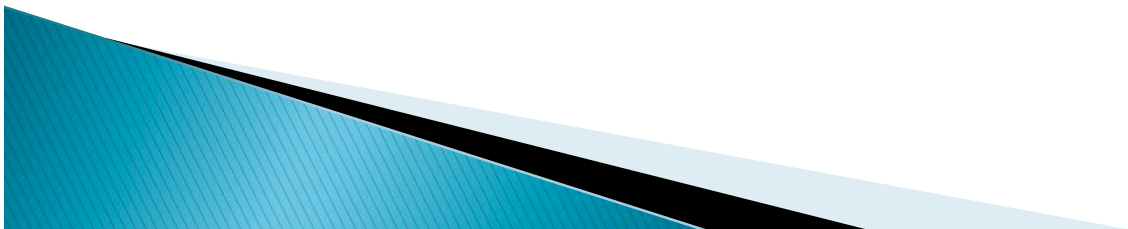
Click the next slide for the correct answer



Quiz Time!

10. It's OK to use someone else's password to access ePHI if you are both authorized for the same access.

- True
- **False**

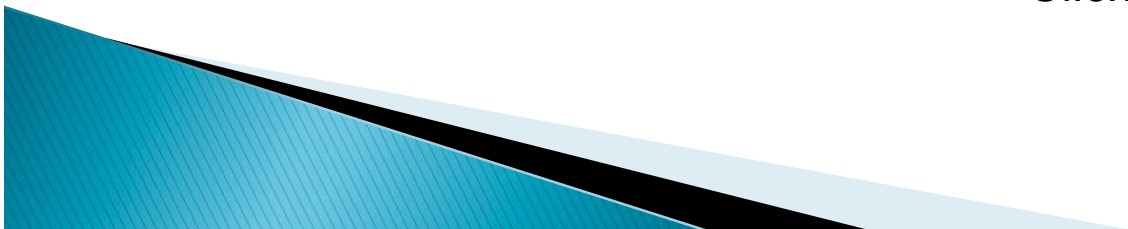


Quiz Time!

11. It's OK to store unencrypted ePHI on a data stick as long as you keep the data stick locked up or in your possession at all times.

- True
- False

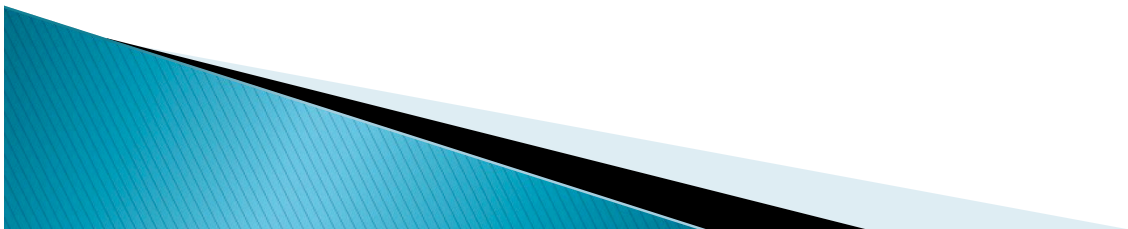
Click the next slide for the correct answer



Quiz Time!

11. It's OK to store unencrypted ePHI on a data stick as long as you keep the data stick locked up or in your possession at all times.

- True
- **False**



Training Certification

- ▶ When you have completed this training please print this page and fill in the following information, sign, and give to your supervisor. By signing you are certifying that you have completed the entire Information Security Awareness Training.
- ▶ Disclaimer: This module is intended to provide educational information and is not legal advice. If you have questions regarding the privacy / security laws and implementation procedures at your facility, please contact your supervisor or the healthcare privacy officer at your facility for more information.

- ▶ Name (please print): _____

- ▶ Job Title: _____

- ▶ Department/Unit: _____

- ▶ Date training completed: _____

- ▶ Signature: _____

- ▶ Employee's home department (or IRB for researchers) must retain this certification or the equivalent for six (6) years as part of required HIPAA training documentation

