University of California
San Francisco
advancing health worldwide™

Advanced HIPAA Healthcare Provider

UCSF University of California San Francisco

Advanced Training

- **This advanced module will cover very specific topics relevant to healthcare providers, and therefore requires you to have foundational privacy and security training (including the concepts below) before proceeding.**
  - Protected health information (PHI)
  - Minimum necessary
  - Disclosures for treatment, payment and operations
  - Privacy breach reporting requirements
- **If you do not have such foundational training, please exit the course and complete the HIPAA 101 module in the UC Learning Center.**
- **Once completed, please re-launch this course.**

UCSF
University of California
San Francisco

Objectives

- Understand your role as a healthcare provider in maintaining privacy of protected health information for: patient care, teaching, research, fundraising, marketing and media
- Provide case scenarios to illustrate the concepts presented in this module
- Learn how to protect the security of patient protected health information

Key Concept: What is PHI?

- **As a reminder, Protected Health Information (PHI) is essentially individually identifiable health information**
  - Health information (e.g., test results) + at least one identifier = PHI
- **To render PHI de-identifiable, you must remove <u>all</u> 18 identifiers**
  - Including “any other unique identifying number, code, or characteristic”

UCSF
University of California
San Francisco

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

UCSF University of California San Francisco

Scenario: PHI vs. De-Identified Data

Question: You are planning to present a case study at a national conference. The subject of the case study suffered extreme brain trauma after his plane crashed near San Francisco. You will not reference the patient's name or date of birth. Do you need to obtain your patient's consent to discuss his case at the upcoming conference?

A. No, because I am sharing this information for educational purposes.

B. No, because I have sufficiently de-identified the information.

C. Yes, because of the unique circumstances of the case, someone can likely re-identify the patient.

D. Yes, because I need a patient's consent whenever I use their information for any purpose.

UCSF
University of California
San Francisco

Answer: PHI vs. De-Identified Data

Answer:

A. No, because I am sharing this information for educational purposes.
Incorrect. PHI discussed during *internal* UCSF teachings (e.g., resident training) is covered under the Terms and Conditions signed by all patients, and therefore wouldn't require patient authorization. However, if the PHI is further disclosed to an external (non-UCSF) audience, such as this scenario, patient authorization would then be required.

B. No, because I have sufficiently de-identified the information.
Incorrect. If there is any unique identifying number, code, or characteristic that could possibly identify the subject of the health information, it is considered PHI, and would require patient authorization before disclosing it to an external audience.

C. Yes, because of the unique circumstances of the case, someone can likely re-identify the patient.
Correct!

D. Yes, because I need a patient's consent whenever I use their information for any purpose.
Incorrect. There are many purposes where patient consent is NOT required before using their information, such as for treatment. It is recommended that you review the HIPAA 101 module and then return to this module.

Teaching Activities: Internal

- You CAN use PHI for teaching UCSF students/residents or other workforce members
  - Includes discussing cases at rounds or in the classroom
  - Minimum necessary still applies so do not share identifiers unless necessary
- You CANNOT use PHI for any teaching outside of UCSF or to non-UCSF audiences without patient authorization
  - Excludes: situations such as giving a lecture at UCSF with non-UCSF people in the audience
- Do not include PHI on handouts
  - Instead de-identify the information or use a projector during the presentation to eliminate the need for a handout
  - If you must include PHI on handouts, collect the handouts after the teaching activity is finished

Teaching Activities: External

External Teaching Activities

- You must use de-identified information or obtain written prior authorization from the individuals whose health information you want to use
- You can disclose PHI to students from another academic institution for teaching purposes, as long as the student has an educational relationship with UCSF
- Other alternative is to use a Limited Data Set (more information in next slides)

De-Identified Data vs. Limited Data Set

- Whereas de-identified data excludes all 18 identifiers, a Limited Data Set includes only dates and zip codes as identifiers
- HIPAA allows the use of a Limited Data Set for teaching, research and public health activities
  - However, if a Limited Data Set is used or disclosed outside of UCSF, then the recipient of the data must first sign a Data Use Agreement
- For assistance with Data Use Agreements, contact Industry Contracts Division (ICD) at Industrycontracts@ucsf.edu or (415) 502-1603

UCSF
University of California
San Francisco

Scenario: De-Identified Data vs Limited Data Set

Question: You are participating in a multi-site retrospective research study, which requires UCSF to give a collaborating site patients' zip codes, dates of birth, dates of death, dates of service and health information. No direct identifiers such as name, social security number, address, will be included. What must occur for this data transmission to happen?

A. Collaborating site must sign UCSF's Data Use Agreement.

B. Only IRB approval is required to share the data.

C. Nothing. This involves de-identified data and therefore is not human subjects research.

Answer: De-Identified Data vs Limited Data Set

Answer:

A. Collaborating site must sign UCSF's Data Use Agreement.
Correct! But note, that IRB approval must still be obtained (see next slide).

B. Only IRB approval and waiver of authorization is required to share the data.
Incorrect. The study involves a Limited Data Set and therefore, in addition to IRB approval and the Waiver of Authorization, requires the collaborating site to sign UCSF's Data Use Agreement.

C. Nothing. This involves de-identified data and therefore is not human subjects research.
Incorrect. Because zip codes and dates are included, this is not considered "de-identified".

UCSF University of California San Francisco

PHI and Research

- In order to access, use or disclose PHI for research purposes, you must do the following:
  - Obtain IRB approval; and
  - Obtain a signed HIPAA authorization form from the patient, or the IRB must issue a Waiver of Authorization
- Note: The Informed Consent Form is NOT the same as the HIPAA Authorization. Both forms must be signed by the subject unless you have a combined consent and authorization.
- UCSF IRB contact info:
  - Website: http://irb.ucsf.edu/
  - Phone: (415) 476-1814
  - Email: IRB@ucsf.edu

UCSF
University of California
San Francisco

Research Privacy – Repurposing

Data appropriately obtained for one purpose cannot be repurposed for another without additional review by the IRB

- This means that information obtained during treatment cannot then be used for research without approval
- Data appropriately used for one research study cannot be used in another study without going through the IRB and consent approval process again

PHI Requests from Researchers – Do's and Don'ts

As a UCSF provider and researcher, you may receive requests from other people to help with their research or provide them with access to UCSF's information for research purposes.

If you receive a request from other UCSF workforce members:

- **Do not** disclose your patients' PHI with researchers unless the patient provides a signed HIPAA research authorization to allow this, or if the IRB has granted a waiver of HIPAA research authorization.
- **Do** inform your patients about UCSF sponsored studies:
  - Can provide patients with study informational materials (i.e., letters, flyers, website, brochures)
  - Can suggest which studies might be of interest
- **Do** suggest patients contact the investigators

PHI Requests from Researchers – Do's and Don'ts

If you receive a request from outside entities:

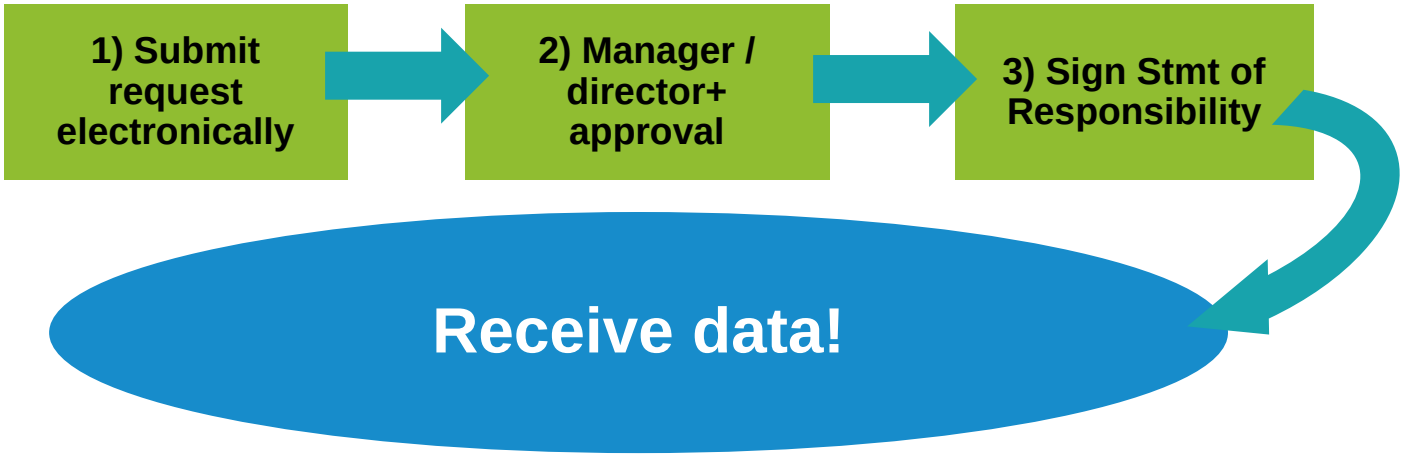
- **Do not** disclose your patients' PHI with research investigators unless the patient provides a signed HIPAA research authorization to allow this, or if the IRB has granted a waiver of HIPAA research authorization.
- **Do** provide the IRB the study protocol for informal review prior to informing your patients about an outside research study
  - IRB, Privacy, Legal Affairs, and Risk Management will need to review the communication prior to its release to patients

Accessing Clinical Systems

- You may only access clinical systems for UCSF business reasons (e.g., patient care, quality improvement)
  - Do not use your access for personal reasons, such as accessing records of a family or friend
  - Please remember that APeX access is tracked and monitored for all users
- While you are permitted to access your patients' PHI for treatment and/or quality improvement purposes, you cannot repurpose the data for research without the following:
  - IRB approval
  - Patient HIPAA research authorization form or Waiver of Authorization

Accessing Clinical Systems

- The process for obtaining PHI/PII for research, operations, business and/or clinical/quality purposes is centralized through ServiceNow. As such, if you need a PHI/PII data set for any of the above purposes, you must:
  - Submit a ticket in ServiceNow
  - Obtain required approvals
  - Sign Statement of Responsibility



Scenario: Access to Medical Records

Question: Your friend's spouse is in the hospital after an accident. Your friend asks you to review what treatment has been provided to the spouse and see if you concur. What are you able to do under HIPAA?

A. Access the person's chart so that you can communicate with your friend about the patient's condition.

B. Contact the charge nurse on the floor and ask her to look into the patient records for you.

C. Advise your friend that you can only look at the medical records if you are treating the patient. Suggest to your friend that he/she request the patient's records and then give it to you for review.

Scenario: Access to Medical Records

A. Access the person's chart so that you can communicate with your friend about the patient's condition.

Incorrect. You may only access UCSF's clinical systems for UCSF business purposes only. Do not access the medical records of your friend, family member, co-worker or VIP for personal reasons.

B. Contact the charge nurse on the floor and ask her to look into the patient records for you.

Incorrect. The charge nurse may only access/disclose information for Treatment, Payment, Operations, or as authorized by the patient. You should contact your friend to get updates on his/her spouse's condition.

C. Advise your friend that you can only look at the medical records if you are treating the patient. Suggest to your friend that he/she request the patient's records and then give it to you for review.

Correct!

UCSF Employees Treated at UCSF

Because of UCSF's excellence and reputation, many UCSF workforce members choose to receive care here. When treating these patients you may need to take added precautions to protect their privacy, and be extra conscious of your actions in regards to communicating about their care.

- **When treating a UCSF workforce member (or are one yourself) review their proactive privacy options:**
  - Enable Break The Glass (BTG) on the employee's medical record in APeX (contact the Admitting Department)
  - Opting out of the facility directory (contact the Admitting Department)
  - Requesting restricted communications (contact Patient Relations)

UCSF Employees Treated at UCSF

- **Be aware that UCSF workforce members can often "wear different hats," and be sure to treat them based on the role for which you are interacting with them. Use appropriate channels of communication; do not comingle**
  - Health care provider ← → patient
  - Colleague ← → Colleague
- **When communicating about these patients with others at UCSF limit the:**
  - Topic: what is necessary for treatment purposes
  - People: those involved in a patient's care
- **Be cognizant of the fact that patient's expectations and comfort levels may change so do not create bad precedent that may cause issues in the future**

Scenario: UCSF Employees Treated at UCSF

Question: A UCSF employee in your department is also a patient of yours. You need to update him/her on his/her test results. Which is the LEAST appropriate method for communicating the test results to the patient?

A. Send message via patient portal (e.g., MyChart)
B. Send secure email from your UCSF email account to the patient's email address listed in their medical record
C. Placing a copy of the test results in the employee's inbox at work
D. Contact the patient using the phone number listed in their medical record

Answer: UCSF Employees Treated at UCSF

A. Send message via patient portal (e.g., MyChart)

Incorrect. This is the preferred method of electronically communicating with patients.

B. Send secure email from your UCSF email account to the patient's email address listed in their medical record

Incorrect. As long as you send the email securely, this method of communicating test results is compliant with privacy rules and policies.

C. Placing a copy of the test results in the employee's inbox at work

Correct, this is the LEAST appropriate method, as their inbox is an employee communication channel, and should not be used to communicate with them in their patient role

D. Contact the patient using the phone number listed in their medical record

Incorrect. This is another preferred method for communicating test results to patients.

UCSF
University of California
San Francisco

Psychotherapy Notes

Disclosures of psychotherapy notes requires the patient's Authorization, except in these situations:

- Use by the originator of the notes for treatment purposes;
- Use or disclosure by UC for its own mental health training programs;
- Use or disclosure by UC to defend itself in a legal action or other proceeding brought by the individual;
- Use or disclosure that is required or permitted with respect to oversight of the originator of the notes.

Psychotherapy Notes: notes recorded by a mental health professional documenting or analyzing the contents of a conversation during a private counseling session or a group, joint, or family counseling session and that are separate from the rest of the medical record

UCSF
University of California
San Francisco

Incidental Disclosures

Incidental disclosures of information are not considered breaches as so long as reasonable safeguards are used to protect PHI and the minimum necessary standard is applied

- "Incidental" means a use or disclosure that cannot reasonably be prevented, is limited in nature and occurs as a by-product of an otherwise permitted use or disclosure.
- This is the law's way of acknowledging that there are limitations to privacy protections as they function in the real world
- Example:
  - Discussions during teaching rounds overheard by neighboring patients
  - Calling out a patient's name in the waiting room
  - Patient seeing a sign-in sheet

UCSF University of California San Francisco

Patient Rights

HIPAA affords patients certain privacy rights. If a patient requests to exercise any of these rights (except for receiving an NPP) do not accept or reject their request. Instead please direct them to Patient Relations

- Receive a Notice of Privacy Practices
- Right to request access a copy of their PHI
- Right to request an amendment of their health record
- Right to an accounting of disclosures
- Right to request restricted disclosures
- Right to request confidential communication
- Right to complain about a violation of rights

UCSF University of California San Francisco

Scenario: Use of Social Media

Question: Your family has a private Facebook group that you use to stay in touch and communicate about events in your life. You recently lost a patient and you want to share this experience and your thoughts with your family to get their support. 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 family.

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

UCSF University of California San Francisco

Answer: Use of Social Media

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 family.

Incorrect. Your family likely knows your place of work and your occupation. When linked with your posting, this provides additional details that may identify the patient. Without the patient's authorization, sharing their PHI is a violation of their privacy.

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

Correct!

UCSF
University of California
San Francisco

Use of Social Media

Be cautious when using social media. Health information published on social media can often be traced back to patients and can result in breaches

- Posting PHI online 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
  - Often the instances that most affect us, and therefore trigger social media posts, are the unique cases
  - These types of cases are more likely to trigger media attention and therefore make the information you post more identifiable
- Inappropriate use of social media has resulted in investigations and penalties by oversight agencies
- Refer to UCSF's Social Media Best Practices: http://www.ucsf.edu/about/social-media-overview/social-media-best-practices

UCSF University of California San Francisco

Scenario: Photo Publication

Question: You participate in a clinical image sharing app with other providers to share unique images and clinical cases. Your patient has a very interesting rash on his back, and you'd like to share it on the app. Which of the following statements is true?

A. The app is a secure environment to post these images because the app members are clinical providers and have a legal obligation to protect PHI
B. As long as you do not include the patient's direct identifiers, face or a unique tattoo in the image, the image is considered de-identified
C. You need to obtain the patient's authorization to post the photo in the app. If even one person can identify the image (e.g., patient's spouse), the image is considered PHI.
D. You must set your profile to private, and only allow your UCSF colleagues access to view your photos, before uploading the image to the app.

UCSF
University of California
San Francisco

Answer: Photo Publication

A. The app is a secure environment to post these images because the app members are clinical providers and have a legal obligation to protect PHI
Incorrect. Regardless of whether the other app members are providers or not, the other members may include non-UCSF providers and/or do not have a treatment relationship with the subject of the image. Patient authorization would be required to upload the photo to the app.

B. As long as you do not include the patient's direct identifiers, face or a unique tattoo in the image, the image is considered de-identified
Incorrect. Because the rash is so unique, it might be identifiable to at least one other person (e.g., patient's spouse).

C. You need to obtain the patient's authorization to post the photo in the app. If even one person can identify the image (e.g., patient's spouse), the image is considered PHI.
Correct!

D. You must set your profile to private, and only allow your UCSF colleagues access to view your photos, before uploading the image to the app.
Incorrect. Even if you restrict access, the images are on the app's server, and therefore UCSF would need a Business Associate Agreement and other contracts to ensure the app company adequately protects the privacy and security of the clinical images.

Risks of Hard Copy PHI Notes

Even in today's electronic world, hard copy records are often needed to facilitate efficient patient care. However, along with that need comes risk:

- Paper documents are misplaced and/or fall out of pockets/bags
- Car thefts are on the rise and can result in stolen PHI
- Often times, these paper documents contain very sensitive information

UCSF
University of California
San Francisco

Provider Notes – Best Practices

- Do not take hard copy notes/PHI offsite
  - Shred the documents before leaving the facility
  - Scan the documents to yourself for remote access
- De-identify the notes
  - Use initials instead of full name
  - Do not reference UCSF on document
- Print/write notes on brightly colored paper, so you can always locate it
- **Treat PHI like it's an infant:** Keep the documents on you at all times – do not leave them unattended in your bag, briefcase or car (even if they're locked in the trunk)

Scenario: Accessing PHI From Home

Question: You are running late for a Warriors game and don't want to miss tipoff but haven't finished everything you need to get done today. You decide to finish the work at home after the game. One of the things you need to do is review patients' charts. Which of the following actions are appropriate?

A. Access APeX remotely from home via UCSF's Virtual Private Network (VPN)
B. Print the documents and keep them in your briefcase hidden in your locked trunk while you go to the game
C. Securely email the PHI to yourself and access it from your computer at home
D. All of the above
E. A & C

Answer: Accessing PHI From Home

A. Access APeX remotely from home via UCSF's Virtual Private Network (VPN)

Incorrect. While this is true, the better answer is E.

B. Print the documents and keep them in your briefcase hidden in your locked trunk while you go to the game

Incorrect. You should refrain from taking PHI offsite, but if you absolutely must, do not leave it unattended – keep it on you at all times.

C. Securely email the PHI to yourself and access it from your computer at home

Incorrect. While this is true, the better answer is E.

D. All of the above

Incorrect. A and C are correct, but not B.

E. A & C

Correct!

UCSF
University of California
San Francisco

Fundraising

- Before engaging in **fundraising** activities, consult with the University Development and Alumni Relations (UDAR)
  - UCSF Campus Policy 450-13 establishes fundraising authority with UDAR
  - Fundraising requires additional patient approval and record keeping, and specific protocols for sharing patient names and MRNs with UDAR
  - Contact UDAR at: giving@ucsf.edu or (415) 476-6922
  - If someone outside of UCSF or UDAR approaches you about fundraising, direct them to UDAR

UCSF
University of California
San Francisco

Communications and Media

- If you need to use PHI for healthcare/educational communication purposes (e.g., sending communications to patients about new technology at UCSF), the communication must be coordinated with University Relations
  - Contact Medical Center Marketing at: (415) 353-4830
  - If UCSF receives payment for the communication, then patient authorization must be obtained and the authorization must state that payment was received for the communication

- On occasion media outlets are interested in UCSF patients
  - You should consult with University Relations prior to speaking with media
  - For use of PHI for any news media, all patients must be consented by University Relations prior to any mention of their name or situation to reporters or news outlets
  - Contact University Relations at: (415) 502-6397

UCSF
University of California
San Francisco

INFORMATION SECURITY

Electronic PHI: Encryption

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

- UCSF Policy requires that any electronic device used for UCSF business be encrypted
  - You may be held liable for breaches caused by PHI on personal unencrypted devices
- Encryption is the only federally recognized method for securing ePHI
- For assistance with encryption, contact the IT Service Desk at (415) 514-4100
- For guidance to install encryption on your personal device: https://it.ucsf.edu/encrypt

Secure Email

All emails containing PHI sent outside UCSF should be sent using the UCSF secure email system

- Note: The best practice for electronically communicating with a UCSF Medical Center patient is to use MyChart
- To secure your UCSF email message, start the subject line with one of the following trigger words:
  - ePHI:
  - PHI:
  - Secure:
- Be sure to include the colon (:)
- This will secure the email even if the recipient forwards or replies to the message
- Instructions available at: https://it.ucsf.edu/services/secure-email/additional/send-secure-email
- If a patient doesn't want to receive secure emails, and requests unencrypted email communications, **you must**:
  - Notify the patient of the risks of sending unencrypted emails; and
  - Document the patient's preference for unsecured email as a note in APeX

Credential Sharing

Each UCSF workforce member is given a unique username and has their own password. This information may not be shared with anyone else. People who need to delegate tasks to others can do this in ways other than sharing credentials:

- To delegate tasks to others, provide their unique ID with the minimum access needed to perform the tasks and remove that access when it is no longer needed.
- For example, to delegate access to a folder in Outlook, right click on the folder, click on “Sharing Permissions” and then add the user to the folder and provide the appropriate level of access. Remove the access when it is no longer needed.

UCSF
University of California
San Francisco

Active Sync

Active Sync provides a secure way to view email on handheld devices. All Active Sync devices are subject to forced device encryption and the UCSF-wide mobile device security standard.

- Active Sync allows for remote wiping of a device if it is lost or stolen (*Remote wiping may result in the possible loss of personal data on the mobile device. Prevent permanent loss of data; back up your mobile device regularly!*)
- Detailed instructions on how to put Active Sync on to your device are available at: https://it.ucsf.edu/services/email-mobile-access

For additional training on IT Security Topics, please go to: https://it.ucsf.edu/services/outreach

UCSF
University of California
San Francisco

Privacy Do's and Don'ts

- DO treat all patient information as if you were the patient. Don't be careless or negligent with PHI in any form, whether spoken, written or electronically stored.
- DON'T take PHI off-site, where possible. If you must take PHI off-site, de-identify and/or never leave it unattended in your bag, briefcase or your car (even if it's locked in the trunk). **You are responsible for securing PHI taken off-site and keeping it in your direct possession at all times.**
- DON'T post any information about your patients (including photographs) on social media or public outlets without prior authorization
- DON'T access patient records for personal reasons (e.g., to check on a friend or family member's health status)
- DO shred or properly dispose of documents containing PHI—do not place in the recycle or trash bin
- DO discuss PHI in secure environments, or in a low voice so that others do not overhear the discussion.

UCSF
University of California
San Francisco

HIPAA Do's and Don'ts (cont.)

- DO encrypt all mobile and electronic devices (e.g., laptops, tablets, mobile phones, thumb drives) used for UCSF business, whether personal or UCSF-owned.
- DO use automatic locks on laptop computers and smartphones and log off after each time you use a computer. Purge PHI from devices as soon as possible.
- DO use secure networks for e-mails with PHI and add a confidentiality disclaimer to the footer of such e-mails.
- DON'T share passwords.
- DO use secure email to send PHI via email.
- DO contact the Privacy Office if you have any questions

UCSF
University of California
San Francisco

Thank you!

- Help us to improve privacy/security of protected health information (PHI).
- Report suspected or known improper disclosures of PHI so UCSF can meet its obligation to mitigate consequences.
- Contact UCSF Privacy Office at (415) 353-2750 for more information on HIPAA or visit our website:

http://hipaa.ucsf.edu

UCSF
University of California
San Francisco

Completing This Course

When you close this window, you will be asked if you have completed this course.

By clicking yes, you indicate you have reviewed these materials and agree to comply with the rules and policies described in the **Advanced HIPAA Healthcare Provider** Module and/or will contact your manager or the UCSF Privacy Office with questions..