March 9, 2010

HIPAA Privacy and Security Training

California State University

Elizabeth Marks
Kathleen Murray
Agenda

- Why HIPAA privacy and security training is important
- HIPAA privacy training
- HIPAA security training
- HIPAA breach notice rules
- HIPAA sanction policy
Why HIPAA training is important
Why HIPAA training is important to you and CSU

- You may interact with employees in many different capacities that involve discussions about medical and other sensitive employee information that needs to be safeguarded

- For example
  - Employees may willingly share information with you about their own health problems
  - Employees may ask you to help them solve problems relating to how a health or dental claim is being handled by an HMO or insurer
  - You may get involved in discipline, workers’ compensation, FMLA, or disability issues that involve private medical information

- The training will explain CSU’s obligations under the HIPAA Privacy requirements that apply to protected health information relating to employee health plans, and it will also reinforce the importance of maintaining the privacy of any sensitive employee information
# Penalties and enforcement

## New civil penalties

<table>
<thead>
<tr>
<th>TYPE OF VIOLATION</th>
<th>PENALTY</th>
<th>Before HITECH</th>
<th>After HITECH – Effective February 2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>Each violation</td>
<td>All such violations of an identical provision in a calendar year</td>
<td>$100</td>
<td>$100 - $50,000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$25,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Due to any type of violation</td>
<td>$100</td>
<td>$100 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Due to unknowing violation</td>
<td>$100</td>
<td>$100 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Due to reasonable cause but not willful neglect</td>
<td>$1,000 - $50,000</td>
<td>$1,500,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Due to willful neglect that is timely corrected</td>
<td>$10,000 - $50,000</td>
<td>$1,500,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Due to willful neglect if not timely corrected</td>
<td>$50,000</td>
<td>$1,500,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>
Penalties and enforcement
New enforcement

<table>
<thead>
<tr>
<th>CRIMINAL PENALTIES</th>
<th>Then</th>
<th>Now</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clearly applicable to individual employees (not just the entity)</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Penalties</td>
<td>Fines $50,000 - $250,000 1-10 years imprisonment for “knowing misuse”</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OTHER CONSEQUENCES</th>
<th>Then</th>
<th>Now</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bad publicity</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Negative employee relations</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Damage to business relationships</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
HIPAA Privacy Training Agenda

- HIPAA Privacy overview
- Uses and disclosures of protected health information (PHI)
- Best practices for safeguarding PHI
- Individual rights
- HIPAA Privacy Official
- Notice of privacy practices
The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

- HIPAA “administrative simplification” regulations govern the privacy and security of individual medical information used, transmitted, and retained by employer health plans and other covered entities, and the electronic transfer of certain health data.

- These regulations cover the following areas:
  - **Privacy** - rules that safeguard the privacy of individuals’ health information by placing limits on its use and disclosure.
  - **EDI** - rules that standardize transactions/code sets for electronic data interchange (EDI) to encourage commerce in health care.
  - **Security** - rules that require the confidentiality and integrity of electronic data, prevent unauthorized access to data, and guard against physical hazards.
Protected health information (PHI)
What is the definition of PHI?

- **PHI** is at the center of the HIPAA Privacy Rule. The rule closely regulates how PHI is used, disclosed, transmitted, and retained. The rule also gives individuals certain rights with respect to their PHI.

- **PHI** is health information that . . .
  - Is created, received, or maintained by a covered entity, **and**
  - Includes “individual identifiers” that clearly identify an individual (or has components that reasonably could be used to identify the individual), **and**
  - Is related to a past, present, or future physical or mental health condition, or the provision of, or payment for, health care (new: genetic information)
Protected health information (PHI)
What are “individual identifiers”?

- What identifiers make health information PHI?

- Any combination of data could identify the individual who’s the subject of the information:
  - Name
  - SSN
  - Date of birth
  - Date of hire
  - Dates of service
  - Telephone or fax numbers
  - Email address
  - Medical record number
  - Health plan beneficiary number

- Geographic identifiers smaller than a state
- Certificate/license numbers
- Vehicle identifiers
- URLs
- IP address numbers
- Biometric identifiers
- Photographic image
- Other unique identifying numbers or codes
Protected health information (PHI)
What form does PHI take and where is it found?

What form can PHI take?
- PHI can be any communication format:
  - Print
  - Electronic (including email)
  - Oral

When will you interact with PHI?
- Benefit staff frequently come into contact with PHI during:
  - Assisting employees with claims ("customer service")
  - CSU oversight of health plans
  - Response to requests for health information
**Protected health information (PHI)**

What’s not considered PHI?

- Private medical information that’s obtained from the employee or health care provider (but not from the health plan) for disability or employment purposes, such as
  - Short-term or long-term disability claims
  - Life insurance
  - Disability pensions
  - FMLA or other types of leave
  - Workers’ compensation
  - Americans with Disabilities Act (ADA) compliance
  - 401(b) medical hardship withdrawals

- The HIPAA Privacy rule does not apply to employer interaction with these types of personal medical information

- However, other laws do protect private medical information
Protected health information (PHI)
What is (and is not) PHI?

Private medical information that relates to FMLA, workers’ compensation, or ADA, including health information maintained as part of employment records in CSU’s role as employer is not covered by HIPAA, but still must be protected.

PHI is health information that relates to a person’s medical condition, the provision of medical care, or the payment of medical care, and that is:
- Individually identifiable, and
- Created, received, or maintained by the health plans.
What is a HIPAA covered entity?

- A HIPAA “covered entity” is a health plan, health care provider, or health care clearinghouse
  - Health plans, such as
    - Group health plans sponsored by CSU or PERS
    - EAPs
    - Health care reimbursement account
  - Health care providers such as doctors, hospitals
  - Health care clearinghouses that assist in transmission of ePHI
- Covered entities must comply with the standards set in the HIPAA Rule
What benefits are affected by HIPAA?

- HIPAA applies to CSU’s health plans offered to employees, COBRA participants, retirees, and their families that provide or pay for:
  - Medical
  - Dental
  - Vision
  - Prescription drugs
  - Employee assistance plans
  - Health care reimbursement account (HCRA)
  - Certain wellness programs
  - Long term care

- Privacy rules apply to both insured and self-funded arrangements
What is CSU's responsibility under HIPAA privacy?

- CSU is responsible for complying with HIPAA privacy rules for its self-funded health plans, including EAPs and HCRA
  - Obtain business associate agreements

- CSU has limited responsibility for fully insured plans and HMOs
  - Insurers/HMOs are responsible for complying with privacy rules for insured health plans
  - However, insurers won’t release PHI to CSU without individual authorization or formal assurances from CSU that CSU will protect PHI
An employee calls to discuss her upcoming hospitalization for heart condition tests with Joe, a CSU campus benefit officer who performs health plan administrative functions. The employee asks Joe to help her with the required pre-certification from the HMO. The HMO provides Joe with details of the surgical procedure that extend beyond the information originally given by the employee.

**Question:** Is the information Joe received from the HMO considered PHI?

**Yes** or **No**
The correct answer is **Yes.**

PHI in any form, even oral communication, relating to future treatment of a medical condition that clearly identifies an individual is PHI if it is received from the health plans.
HIPAA Privacy Training
Uses and Disclosures of PHI
Who has access to PHI?

- CSU staff responsible for administering health plans, but only to perform certain administrative functions (e.g. assistance with customer service, claims questions, data analysis)
- “Business associates” that perform services for the plans and have signed Business Associate Agreements
- Insurers and HMOs with respect to the plans they insure
When PHI can be used

- PHI can be used or disclosed for any purpose if the participant specifically permits the use or disclosure in a HIPAA Authorization.

- A HIPAA Authorization is generally not required to use PHI for:
  - Enrollment activities
  - Normal administration of the health plans:
    - Payment activities (e.g. HCRA claims), or
    - Health care operations (e.g. audits, customer service, vendor performance reviews)
  - Obtaining premium bids and making plan amendments if only “summary health information” is used

- CSU employees must follow policies and procedures that satisfy the HIPAA Privacy standards when using PHI.
When PHI cannot be used

Any other time!
Important definitions

- **Disclosures** – The release, transfer, or provision of access to, or divulgence in any other manner of PHI to parties *outside* the covered entity holding the information.

- **Use** – The sharing, employment, application, utilization, examination, or analysis of PHI *within* the covered entity that maintains such information.

- **Minimum necessary** – Covered entities must make reasonable efforts to use, request, and disclose a ‘limited data set’ of PHI unless more elements are needed to accomplish the task.

- **Limited data set** – A limited data set is PHI that *excludes* the individual identifiers.
What information can business associates and insurers share with CSU?

- Enrollment/disenrollment information
  - Processing of annual enrollment selections
    - New hire benefit selections
    - Enrollment changes
    - Eligibility questions

- Summary health information (all individual identifiers removed)
  - Obtain premium bids for coverage
  - Modify, amend, or terminate the plan

- Information related to plan administration activities
  - As long as CSU promises to protect the PHI via a HIPAA amendment)
As required by the HIPAA Privacy Rule, CSU has identified that HR and benefits are the only staff with access to PHI.

HR and benefits staff must follow procedures to:
- Limit disclosures of and requests for PHI to the “minimum necessary” for the intended purpose.
- Maintain procedures for storage of PHI.
- If feasible, return or destroy PHI received from the plan and follow procedures for PHI that isn’t returned or destroyed.

HR and benefits staff will not use PHI obtained as the result of health plan administration for employer functions (such as processing disability or life claims) unless they have written authorization from the plan participant.
Non-plan administration activities

Individuals who are not identified to perform health plan administrative functions must have a written HIPAA Authorization from the plan participant to receive PHI from the health plan.

PHI will not be used or disclosed on the basis of a written HIPAA Authorization, unless it is verified that the Authorization:

- Has not expired,
- Has not been revoked, and
- Includes all required information.

A copy of each Authorization will be retained for six years from the later of the date the authorization was created or the last date the authorization was effective.
Disclosure to others acting on behalf of the participant

- Participants can generally obtain their own PHI without a HIPAA Authorization.

- A participant’s PHI may, and in some situations must, be provided to certain others without a HIPAA Authorization as follows:
  - Persons considered to be the participant’s legal “personal representative” must be treated the same as the participant (including for purposes of individual rights in the next section).
  - Family members, friends, and others who are not a personal representative, if identified by the participant and involved with the participant’s care or payment for care and
    - The participant had opportunity to agree or object to the disclosure, or
    - The participant’s incapacity or an emergency makes it impossible to obtain the participant’s agreement.
Who can be a “personal representative”? 

- Personal representatives of a participant who may obtain the participant’s PHI without the need for a HIPAA Authorization generally may include the following:

<table>
<thead>
<tr>
<th>PHI of:</th>
<th>May be shared with:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minor child</td>
<td>Parent or guardian*</td>
</tr>
<tr>
<td>Adult child</td>
<td>Parent or guardian**</td>
</tr>
<tr>
<td>Adult</td>
<td>Spouse or adult**</td>
</tr>
<tr>
<td>Deceased</td>
<td>Executor or administrator**</td>
</tr>
</tbody>
</table>

*proof of relationship required
**proof of legal authority required
Limitations on parent’s status as personal representative

- There are some restrictions on providing PHI to a parent or guardian
  - Minor lawfully obtained the health services with consent of someone other than parent
  - Information sharing would not be in minor’s best interest (endangerment, abuse, neglect)

- Refer to state laws for details
Verify the identity of all persons making requests for PHI

<table>
<thead>
<tr>
<th>Who makes the request</th>
<th>To verify identity. obtain*</th>
</tr>
</thead>
</table>
| Participants, beneficiaries, and others acting on their behalf | • Photo identification  
• Letter or oral authorization  
• Marriage certificate  
• Birth certificate  
• Enrollment information  
• Identifying number  
• Claim number |
| Health plans, providers, and other covered entities         | • Identifying information about the purpose of the request  
• Identity of a person, business, address, phone number, and/or fax number |
<table>
<thead>
<tr>
<th>Who makes the request</th>
<th>To verify identity, obtain*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public officials</td>
<td>• For in-person requests, agency identification, official credentials, or other identification, or other proof of government status</td>
</tr>
<tr>
<td></td>
<td>• For written requests, on appropriate letterhead, and written statement of legal authority</td>
</tr>
<tr>
<td>Person acting on behalf of a public official</td>
<td>• Written statement on government letterhead or other evidence of agency</td>
</tr>
</tbody>
</table>
Verify the identity of all persons making requests for PHI (continued)

<table>
<thead>
<tr>
<th>Who makes the request</th>
<th>To verify identity, obtain*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Person acting through legal process</td>
<td>• Copy of the applicable warrant, subpoena, order, or other legal process</td>
</tr>
<tr>
<td>Person needing information based on health or safety threats</td>
<td>• Consult with the Privacy Official</td>
</tr>
</tbody>
</table>
Information that is NOT individually identifiable can be used or disclosed at any time, without restrictions.

Such information is referred to as “de-identified” information.
CSU staff can disclose as much PHI as they like in the course of performing plan administrative functions.

**True** or **False**
Quiz Answer

The correct answer is **False**.

CSU’s workforce staff must always take measures to limit the uses and disclosures of PHI to the minimum necessary to accomplish the intended purposes of a plan administrative function.
HIPAA Privacy Training
Best Practices for Safeguarding PHI
Best practices for protecting PHI

- When using or disclosing PHI, the plan must make reasonable efforts to use or disclose the least amount of PHI reasonably necessary to accomplish the intended purpose of the use, disclosure, or request; use de-identified information whenever possible.

- The plan must make reasonable efforts to prevent uses and disclosures not permitted by the plan’s Privacy and Security policies and procedures.

- PHI in any medium, including paper, electronic media, oral or visual representations must be protected by physical and technical safeguards.

- When a person calls for assistance on a claim issue that will involve PHI, you must verify identity before taking any other action.
Protecting hard-copy PHI

- Limit photocopies that contain PHI
- Keep a clean desk
- Put away and secure PHI when you leave your desk during the day
- Keep PHI in closed, locked drawers/cabinets when you leave for the day
- Store documents you must keep for a long time in areas with limited access
- Destroy PHI as soon as it is no longer needed
- Shred all paper when no longer required
Protecting email and electronic storage media that contain PHI

- Funnel incoming email through appropriate channels to limit the number of people who have access to PHI
- Limit use of PHI in emails (avoid forwarding email strings that contain PHI; make sure message contains only the minimum necessary)
- Store diskettes, CDs, or tapes in locked rooms or files
- Destroy electronic PHI that is no longer needed (including shredding or destroying disks/CDs)
- Account for the external distribution of electronic media that contains PHI
- Permanently remove PHI from disk drives, diskettes, or tapes that will be reused
- Use locking screensavers to limit access to work stations and laptops
Protecting faxes that contain PHI

- Use fax machines designated for health plan administration
- Use fax cover sheet with confidentiality statement
- Limit faxing of PHI to urgent information only
- Notify receiver that you are sending fax
- Check confirmation sheets to verify fax was received
Protecting oral communication regarding PHI

- Limit discussion of PHI in conversations unless absolutely necessary
- Verify the identity of individuals on the phone before discussing PHI
- Use reasonable measures to prevent others from overhearing conversations (close your door and avoid speaker phone, for examples)
- Restrict voice mail messages to high-level information
Quiz

Question: Which of the following safeguards should be followed for protecting hard-copy PHI?

Choose your answer:

a) Keep a clean desk
b) Keep PHI in closed, locked drawers/cabinets when you leave for the day
c) Destroy PHI as soon as it is no longer needed
d) All of the above
The correct answer is (d).
All of the physical safeguards listed are reasonable measures to take to ensure that hard-copy PHI is kept secure and confidential.
HIPAA Privacy Training
Individual Rights
Individual rights regarding PHI

Basic rights granted by HIPAA Privacy to each person include the right to:

- Access, inspect, and copy PHI that relates to him or her
- Amend PHI if there are errors or omissions
- Request restricted use of PHI
- Require confidential communications
- Require an accounting of non-routine disclosures

All rights may be exercised by an individual to whom the PHI pertains or by his or her designated representative.
Individual rights regarding PHI

- CalPERS medical dental or vision coverage
  - Participant requests (other than requests for restrictions or requests for alternative means or locations for receiving communications of PHI) that pertain to CalPERS medical, dental or vision coverage should be directed to the applicable HMO or insurance carrier.

- HCRA and any other non-CalPERS health benefits
  - The Campus Privacy Contact will have the participant fill out the applicable form and forward it to the CSU Privacy Official. The Privacy Official will respond to all requests.
  - See CSU’s HIPAA Privacy Policy and Procedure Manual for further information.
HIPAA Privacy Training
HIPAA Privacy Official
HIPAA Privacy Official: roles and responsibilities

- CSU’s HIPAA Privacy Official is Michelle Hamilton
- The Privacy Contacts are the campus Benefit Officers
- The Privacy Official is responsible for the HIPAA Privacy compliance process, including:
  - Assessing CSU’s HIPAA Privacy compliance needs
  - Developing and implementing HIPAA-related policies and procedures, including those in the HIPAA Privacy Manual
  - Supervising training for CSU’s staff involved in health plan administration
- Other duties of the HIPAA Privacy Official include:
  - Monitoring ongoing compliance
  - Monitoring resolution and tracking of complaints
  - Determining appropriate actions to take to resolve complaints
  - Answering HIPAA-related questions for CSU’s employees
  - Ensuring that required documentation is maintained and retained for six years
Notice of privacy practices

- Describes CSU’s written procedures for uses and disclosures that are part of CSU’s health plan administration
- Lists uses and disclosures of PHI that the plan can make without an authorization (e.g. responding to a request from a public health agency)
- Describes CSU’s process for handling participant requests for PHI, complaints about alleged privacy violations, and other HIPAA individual rights
- Lists contacts with business associates that will provide assistance to plan participants who assert their HIPAA Privacy rights
- Must be given to new participants at enrollment, and to all within 60 days of a material revision
HIPAA Security Training
HIPAA Security Awareness Training

- The security regulations (HIPAA Security Rule) generally require employers who sponsor group health plans to take appropriate precautions to secure their health plans’ electronic protected health information.

- We are providing this Security Awareness Training to educate you on the general provisions of the HIPAA Security Rule and to apprise you of the basic precautions you will be expected to observe to assist CSU in satisfying its responsibilities under the regulations.

- Should you have any questions about this training course, or your participation in it, please contact your HIPAA Security Official.
What will be covered in this training?

This course will discuss the following subject areas:

- How this training relates to you
- Overview of the HIPAA Security Rule
- Three areas that the HIPAA Security regulations indicate are critical in maintaining the security of electronic Protected Health Information (e-PHI)
  - Minimizing the introduction of malicious computer software
  - Proper use of system user names
  - Creating and maintaining robust passwords
- Additional responsibilities for e-PHI users
Why is HIPAA Security Awareness Training mandatory?

Because you are an employee who has access to computer equipment or software containing protected health information related to CSU’s health plans, the HIPAA Security Rule requires that you participate in HIPAA Security Awareness Training to learn about the basic procedures you must follow to protect that information.

Following CSU’s electronic security procedures is important because the procedures help to protect the:

- Confidentiality (only the right people see it),
- Integrity (the information is what it is supposed to be—there has been no unauthorized alteration or destruction), and
- Availability (the right people can see it when needed)
HIPAA Security Training Overview
HIPAA Security Rule

- Electronic PHI (or e-PHI) is PHI:
  - Electronically created;
  - Electronically received;
  - At rest or maintained in a storage device such as a computer hard drive, disk, CD, or tape; or
  - In transit via the Internet, dial-up lines, etc.

  - For example, email FTP (file transfer protocol), EDI (electronic data interchange), IVR (interactive voice response), and fax-back systems used to transmit PHI
HIPAA Security Rule

- e-PHI is not:
  - PHI that was not in electronic form before transmission, such as information shared by:
    - Person-to-person telephone calls,
    - Copy machines,
    - Paper-to-paper fax machines, or
    - Most voice mail
  - De-identified information is not PHI or e-PHI

- The HIPAA Privacy Rule establishes standards for safeguarding e-PHI only
What are the objectives of the HIPAA Security Rule?

- Secure e-PHI at rest, while in the custody of group health plans
- Secure e-PHI in transit, both between health plans
- Protect against reasonably anticipated:
  - Threats or hazards to e-PHI security or integrity
  - Unauthorized uses or disclosures
HIPAA Security Rule Required Policies and Procedures

- The HIPAA Security Rule requires that CSU implement reasonable and appropriate *policies and procedures* governing administrative, physical, and technical safeguards to comply with the HIPAA Security Rule.

- Procedures implemented to comply with the HIPAA Security Rule must be reviewed and modified, as needed, to ensure the reasonable and appropriate protection of e-PHI over time.

- HIPAA Security compliance is an on-going effort that must be constantly monitored.

- You should review CSU’s HIPAA Security policies and procedures for more detail about the safeguards we’ve implemented to protect e-PHI. Contact the CSU HIPAA Security Official for these policies and procedures.
HIPAA Security Training
Critical Security Risks
Critical Security Risks

Three critical security risks must be eliminated or minimized by all CSU staff who have access to e-PHI to ensure the confidentiality, availability, and integrity of e-PHI.

1. Malicious computer software, such as viruses
2. Unauthorized use of system user names
3. Weak or unprotected system and file passwords
Risk 1: Malicious Computer Software

- Malicious computer software:
  - Is designed to damage or disrupt a system
  - Has an intentional negative impact on the confidentiality, availability, or integrity of e-PHI

- Malicious computer software can:
  - Destroy your computer files, or
  - Block your access to critical computer applications
Malicious Software
How does it get on my computer?

- Infected e-mail attachments
- Computer software from non-secure sources
  - Websites
  - Unlicensed software
- Files stored on external electronic storage media
  - Diskettes or CDs could contain malicious software
Malicious Software
Your responsibilities to safeguard against it

- **Be suspicious!** Don’t open e-mails or e-mail attachments that are from suspicious or unknown sources or have suspicious subjects.

- **Report suspicious e-mail** and other potential security incidents to the CSU HIPAA Security Official or IT staff.

- **Comply** with CSU instructions to ensure your work-station virus protection software is kept up-to-date.

- **Read** security alerts released by IT staff on the status of malicious software threats related to e-mails.
Malicious Software
Your responsibilities to safeguard against it

- *Never* copy, download, or install computer software without permission
- *Never* disable or tamper with the virus protection software installed on your workstation and/or laptop
- *Always scan* files from external storage media *before copying* them to detect the presence of malicious software
- *Promptly notify* the IT staff if you become aware of any misuse of CSU equipment, software, or data within CSU
- *Make sure* any home workstation or laptop you utilize for CSU business has up-to-date virus protection software
Security Alerts and Reminders
Why read them?

- **Security alerts** issued by the IT staff contain important information and instructions about how to safeguard against new sources of malicious software threats.

- **Security reminders** contain important suggestions and methods of improving your ability:
  - To safeguard against malicious software threats, and
  - To maintain secure individual system-user names and password.
Quiz

**Question:**
How often should the computer virus software on my workstation or laptop be updated?

**Choose your answer:**
(a) Never. Once installed, it never needs to be updated  
(b) As soon as the updates are available  
(c) Only after a security incident related to malicious software has occurred
Quiz Answer

The correct answer is (b).

Computer virus protection software should be kept as up-to-date as possible in order to ensure that the appropriate safeguards are in place to protect against the new and ever-changing malicious software threats that are present.
Question:
If you receive a security reminder or security alert in your e-mail in-box, you should:

Choose your answer:
- a) Delete it without reading its contents
- b) Immediately open the e-mail, read it, and follow all of the instructions
- c) If you are busy, open and read it later
- d) Follow the instructions, but only if you think they apply to you
Quiz Answer

The correct answer is (b).
The purpose of security reminders and alerts is to assist in preventing malicious software attacks. By paying immediate attention to the instructions contained in the security reminders and alerts the potential of a successful malicious software attack is greatly reduced.
Risk 2: Unauthorized Use of Passwords and/or System User Names

- Keeping your individual system user name and passwords **secure** is essential to maintaining the confidentiality, availability, and integrity of PHI
  - By keeping your user name and password confidential, you help ensure that e-PHI will be maintained correctly
  - Unauthorized use of individual user names compromises e-PHI and defeats the audit trails designed to monitor e-PHI use
- User names for terminated personnel will be disabled immediately
Never Share User Names or Passwords

- Sharing user names and passwords defeats the authorization procedures that have been put in place to control access to e-PHI based on a user’s job responsibilities

- You are responsible for all actions taken with your names
Never Leave A Written Clue
Your responsibilities

- Do not leave information at your workstation, laptop, or desk that could divulge what your system user names and passwords are
  - Never leave any written record of your system user names and passwords near your desk or workstation

- If you have to write them down, keep a record of passwords and system-user names in a secure location away from your desk and/or workstation
  - Never keep a record of your system-user names or passwords in luggage or laptop bags if they are going to be out of your immediate control
Passwords and User Names
Your responsibilities

- Never use another employee’s user name and password
- Never ask another employee to reveal his/her personal user name and password
- You are responsible for controlling your password maintenance!
Quiz: Test Yourself

Question:
In case of emergency, it is a good practice to hide a copy of your user name and password under your workstation keyboard at your desk.

Is this true or false?
The correct answer is false.
You should not leave information at your workstation, laptop or desk that could divulge your system user name and password because it provides easy access to unauthorized persons. If you must keep a record of this information, store it in a secure location away from your desk and/or workstation. Never keep a record of your system user name or password in luggage or laptop bags.
Risk 3: Weak or Ineffective Passwords

- Maintaining secure and strong passwords for systems and files is an essential element in achieving competent security for e-PHI
  - Passwords are your first line of defense for protecting the confidentiality and integrity of systems and files
  - Secure passwords are an essential safeguard against unauthorized use of your system user name or unauthorized access to your files
- To be effective, passwords must be:
  - Private and
  - Difficult to discover
What Makes a Password STRONG?

- It cannot easily be found out
  - 12345, abcde, your name, birthday, or name of your child are *not* strong passwords!

- It contains more than 6 characters

- It contains a random combination of numbers and alphabetic characters
  - G258V74Z is a good example of a strong password
Tips for STRONG Passwords

- Avoid proper names or personal initials
- Avoid real words contained in either English or foreign language dictionaries
- Avoid personal dates of significance, like birth dates or anniversaries
- Never use a repeating pattern of letters and/or numbers
- Never repeat the corresponding user name as part of the password
- Use a combination of numbers and alphabetic characters, for example: A9HZ37YT
Question:
Which of the following is a characteristic of a strong password?

Choose your answer:

a) Contains the employee’s date of birth
b) An easy-to-remember word out of the dictionary
c) A sequential string of either letters or numbers
d) A random combination of numbers and alphabetic characters
Quiz Answer

The correct answer is (d).
Robust passwords consist of a random combination of numbers and alphabetic characters. Passwords comprised of repeating numbers, personal information (e.g., birth date), or common words may be easily guessed.
Steps to Further Safeguard e-PHI

- Take special care to protect portable media like laptops, Blackberries, and computer diskettes:
  - Password-protect the device to prevent access by unauthorized users
  - Keep these items in your personal possession when in public places
  - Do not check them with your luggage when traveling (e.g., on planes, trains, etc.)
  - Keep them in a locked suitcase or safe when in hotels
  - Exit all programs when the device is not in use
Steps to Further Safeguard ePHI

- Store all files containing e-PHI on network drives (rather than on local drives) to ensure the data is routinely backed up. Limit access to the network directory to e-PHI users.

- Include e-PHI in attachments to emails, rather than in the text of the message itself. Password-protected or encrypt the attachment as warranted.
Question:
I don’t need to implement password-protected access to my laptop.

Is this true or false?
Quiz Answer

The correct answer is false.
Access to data on portable media devices, such as laptops and Blackberries, must be password-protected at a minimum to prevent unauthorized users from gaining access to systems containing e-PHI.
HIPAA Privacy and Security Training
Breach notice rules
Breach notice obligations

- Effective 2009, a breach of PHI or ePHI not secured pursuant to prescribed “safe-harbor” standards (difficult to meet) require covered entities to:
  - Within 60 days, notify individuals whose PHI/ePHI is at risk because it was improperly disclosed or accessed
  - Notify the US Department of Health and Human Services of the breach
  - If breach affects 500 or more individuals in a jurisdiction, also notify the media

- Not every unauthorized access or disclosure will require a breach notice
  - Case-by-case evaluation required to see if breach notice rules are applicable

Safe harbor standards for encryption and destruction
At present, most employers have difficulty meeting the “safe harbor” rules for encryption and destruction that would relieve them of the breach notice obligations

Case-by-case evaluation required
Employer must evaluate, case-by-case, whether a specific breach requires notice
HIPAA Privacy and Security Rules
Breach notice responsibilities

- If you are aware of a breach of PHI or ePHI, contact the CSU HIPAA Privacy Official immediately
- Remember: HIPAA complaint and sanction polices apply to breach duties
HIPAA Privacy and Security Training
Sanction Policy
CSU is committed to protecting the PHI and ePHI in our control and that we maintain on behalf of our health plans; we will enforce disciplinary sanctions on those employees who violate the procedures in the HIPAA Privacy and/or Security policies and procedures.

Based on the facts and circumstances of a particular violation, sanctions may range from oral warnings to termination of employment.

If you observe non-compliant behavior or practice on the part of another CSU employee or vendor, you should report it to the CSU HIPAA Privacy Official.

CSU maintains written Privacy and Security policies and procedures for safeguarding PHI and e-PHI as outlined in this training—and you are responsible for complying with these procedures.

HIPAA compliance is EVERYONE’S responsibility!
Congratulations!

- You have completed the HIPAA Privacy and Security training course
- Thank you for participating in this required training