


MERCER
MORRIS | MERCER | HICKL
CLYDE CENTER | CLEVELAND

Building. Sustaining. Inspiring.



HIPAA Privacy & Security Training Part II


Wade Symons, Amy Pavlu
CPEEHCC Training Conference
Las Vegas

Services provided by Mercer Health & Benefits LLC

Agenda

- HIPAA/PHI refresher
- Safeguards for protecting PHI and e-PHI: Practical applications
- Understanding HIPAA's impact through everyday scenarios

Mercer 1



HIPAA/PHI refresher

The Privacy Rule – what it is and who is covered

- **The Privacy Rule applies to:**
 - Health plans, including employer-sponsored health plans
 - Health care providers: doctors, hospitals, etc.
 - Organizations (called Business Associates) who provide services to or on behalf of health plans or providers
- Health Plan = Plan that provides or pays for health care
 - All insured and self-funded employer plans
 - HMOs, insurers, etc.
- Types of benefit plans covered by HIPAA privacy rules include:
 - Medical
 - Prescription drug
 - Dental
 - Vision
 - Long-term care
 - Healthcare FSA
 - Employee assistance plan

Mercer

3

Benefit plans NOT covered by the Privacy Rule

- Life and AD&D insurance
- Workers' compensation and OSHA activities
- Short-term disability and long-term disability
- Return to work activities
- ADA reasonable accommodations
- FMLA leave
- Health-related absences
- Leaves of absence
- Retirement plans

Mercer

4

Protected Health Information (PHI)

Protected Health Information (PHI) is at the center of HIPAA privacy rules. The rules closely regulate how PHI is used, disclosed, transmitted, and retained.

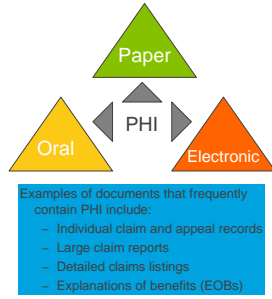
Mercer

5

What is Protected Health Information (PHI)?

Individually identifiable health information that

- Clearly identifies 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, treatment of that condition, or payment of medical benefits, **and**
- Is created or received in any medium (verbal, written or electronic) by a plan or health care provider



Mercer

6

What is not considered PHI?

- Health information in employment records related to, for example:
 - Disability
 - Reasonable accommodations for ADA
 - Worker's compensation
 - OSHA, ADA, FMLA
 - Other leaves of absence

The Privacy Rules do not apply to this type of medical information; because it's not related to the health plan, it's not considered PHI, and, therefore, not protected under HIPAA

Mercer

7

What is electronic PHI (e-PHI)?

- The HIPAA Security Rule contains additional requirements specific to PHI in electronic form
- Electronic PHI (e-PHI) is:**
 - 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, e-mail, FTP (file transfer protocol), EDI (electronic data interchange), IVR (interactive voice response), and fax-back systems used to transmit PHI

Mercer

8

What is electronic PHI (e-PHI)?

e-PHI is NOT...

e-PHI is not:

- **De-identified information**
 - 18 specific identifiers are removed
- **Information that was not in electronic form before transmission**
 - Person-to-person phone calls
 - Copy machines
 - Paper-to-paper fax machines
 - Voicemail



Safeguards for protecting PHI and e-PHI
Practical applications

Your role in safeguarding PHI

Printed/hard copy documentation

If you receive or possess printed/hard copy documentation of plan participants' PHI, consider the following procedures:

- Funnel incoming mail through distinct channels to limit the number of people with access to PHI
- Limit photocopies of PHI
- Keep a "clean desk"
 - Put away PHI if you leave your desk during the day
 - Place PHI in closed and locked drawers or cabinets when you leave the office for the day
- Store documents you must keep for a long time in storage areas with limited access
- Shred PHI in paper format if no longer must be retained

Your role in safeguarding PHI

Faxes

- When faxing PHI for any purpose, consider these guidelines:
 - Use fax machines designated solely for health plan administration
 - Machine should not be located in publicly accessible areas
 - Use fax coversheet with confidentiality statement
 - Limit faxing of PHI to *urgent information only*
 - Notify receiver you are sending fax
 - Check confirmation sheets to verify fax was received

Your role in safeguarding PHI

Oral conversations/telephone calls/voicemail

- Limit discussions of PHI in oral and phone conversations unless absolutely necessary
- Follow procedures to verify the identity of individuals on the phone before discussing PHI
- Use reasonable measures to prevent others from overhearing conversations
 - Do not use speakerphone
- Do not leave voicemail messages containing PHI

Your role in safeguarding PHI

E-mail and electronic storage

- PHI you receive or distribute via e-mail or have on electronic storage also needs to be carefully protected
 - Destroy unneeded PHI
 - Destroy CDs or diskettes so that they are not readable
 - Limit use of PHI in e-mails
 - Do not forward strings of e-mails containing PHI; prepare a new message with only the minimum information necessary

Your role in safeguarding PHI

File retention

- Review your employer's record retention policy
- Retain files containing PHI only if they are actively being used
- Return or destroy files containing PHI when no longer needed

Your role in safeguarding PHI

Verifying PHI requests

- When requests for PHI are received from an employee, plan participant or other individual, you should follow certain procedures to verify the requestor's identity
- Individuals should provide proper identifying documents before you can disclose PHI
- If there is any question in your mind that the person requesting a participant's PHI is not who they claim to be, do not disclose any elements of PHI without asking the participant to complete an authorization form
 - Contact your Privacy Officer if you have questions

e-PHI safeguards

Three critical security risks must be eliminated or minimized by those who perform group health plan functions to ensure the confidentiality, availability, and integrity of e-PHI:

- | | |
|---|---|
| 1 | Malicious computer software, such as viruses |
| 2 | Unauthorized use of system Login ID |
| 3 | Weak or unprotected system and file passwords |

Malicious software

How does it get on my computer?

- Infected e-mail attachments
- Computer software from non-secure sources
 - Web sites
 - Unlicensed software
- Files stored on external electronic storage media
 - Diskettes or CDs could contain malicious software

For these reasons, most employers have strict requirements relating to opening e-mail attachments and downloading software

Unauthorized use

Passwords and login IDs

- Keeping your individual system login ID and passwords **secret** is essential to maintain the confidentiality, availability, and integrity of PHI
 - By keeping your login ID and password confidential, you help ensure that e-PHI will be maintained correctly
- Login IDs for terminated personnel should be disabled immediately

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)
 - 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 e-PHI

- 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 e-mails, rather than in the text of the message itself
 - Password-protect or encrypt the attachment, as warranted



Scenarios

Scenario #1

“What if...”

Bob contacted the insurance carrier after they processed his medical claim at the non-network level, even though he had used a network provider. The insurance carrier customer service representative said they would re-process the claim, but it still hasn't been paid correctly. Bob asks you to help get this claim paid.

- IS THIS PHI? IS THIS e-PHI?
- WHAT SHOULD YOU DO?

Answer

Yes, this is PHI

No, this is not e-PHI

- You can help Bob, but you should only get the minimum information necessary to assist with getting his claim paid
- Be careful about what information you disclose via e-mail
- Distribution should be limited to those who "need to know"

Scenario #2

"What if..."

An employee approaches a manager or general HR staff person, explains that he/she has been struggling with arthritis for several months but some of the expenses for the helpful treatment recommended by his/her physician are not being covered by the Company health plan. The manager submits the matter to HR and asks to be kept advised.

- IS THIS PHI? IS THIS E-PHI?
- CAN THE MANAGER LATER BE ADVISED BY HR WHAT THE PROBLEM WAS, AS WELL AS THE CORRECTION?

Answer

This is PHI

- Although the manager may submit the information to HR, the "minimum necessary" rules require that only those HR personnel authorized to handle PHI be involved in discussions with the insurer and follow-up with the employee
- The manager may receive notice that the matter has been resolved, but no PHI may be shared
- If the information is put into electronic form and then transmitted, it will be considered e-PHI

Scenario #3

"What if..."

Roger calls his manager and tells him that he needs to take a leave of absence because he's been admitted to the hospital and has just had his appendix taken out.

- IS THIS PHI?

- IS IT OK FOR ROGER'S MANAGER TO TELL THE REST OF THE STAFF THAT ROGER IS OUT ON A LEAVE OF ABSENCE?

Mercer

27

Answer

- **No, this is not PHI**
 - It is personal medical information that's obtained for employment purposes
- It is OK for Roger's Manager to tell the rest of the staff that Roger is out on a leave of absence; however, best practices dictate that Roger's Manager should not disclose Roger's specific medical information with other people without Roger's authorization

Mercer

28

Scenario #4

"What if..."

Tom calls you and identifies himself as the spouse of one of your employees. His wife is about to have surgery and he wants to know if her physician has coordinated everything with the insurance carrier as required. You research his request, get the information, and call Tom back. Tom does not answer, so you leave a message on his answering machine with the requested information. You do not make any notes of this event.

- IS THIS PHI?

- HAVE ALL PRIVACY RULES BEEN FOLLOWED?

Mercer

29

Answer

- **Yes, this is PHI**
- You should not have released the PHI without authorization from the participant, unless adequate verification of the relationship was first obtained
- Because you left PHI on the answering machine instead of requesting a call-back, the information is available to anyone with access to the answering machine and so was not properly safeguarded
- Finally, HIPAA requires that an accounting of all "non-routine" disclosures be provided upon request by a participant
 - Unauthorized disclosures are nonroutine, and the failure to record the exchange makes it impossible to provide an accounting if the participant later asks for one
- Since this transaction is all verbal, there is no e-PHI created

Mercer

30

Scenario #5
"What if..."

Nicky has been out sick for four weeks, and returns to work today. She faxes a copy of her doctor's Release Form to show she is approved to return to work with no restrictions.

- IS THIS PHI?
- WHAT SHOULD YOU DO WITH THE RELEASE FORM?

Mercer

31

Answer

- **No, this is not PHI**
 - Sick leave and other disability programs are not covered by the HIPAA Privacy Rule
- However, the Release Form should be kept confidential

Mercer

32

Questions?



Mercer

33

MERCER

SHARSH | MERRICK | KROSSL
SILY | CAMPBELL | CLYDE WYMAN

Services provided by Mercer Health & Benefits LLC