HIPAA Regulations

Overview

HIPAA Regulations Course Introduction

This course on HIPAA Privacy and Security Regulations is for all faculty, staff and student employees at the University of Colorado Denver and University of Colorado Anschutz Medical Campus. You must complete this course within thirty days of hire.

This course will cover:

- The HIPAA Privacy and Security Rules
- Protected Health Information (PHI)
- Storing and protecting health information in person or online
- Finding assistance for HIPAA privacy and security matters

This course will take approximately 25 minutes to complete. There is a 5-question quiz at the end. You must pass the quiz with at least 4 answers (80%) correct to receive credit for taking the course.

HIPAA Regulations

Overview

HIPAA Regulations Course Introduction

We all have information stored electronically that can be accessed in a number of different ways. The privacy and security of our personal information is a concern for all of us.

The **Health Insurance Portability and Accountability Act** (**HIPAA**), is a United States law designed to provide privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals and other health care providers.

Continue to **Module 1: HIPAA Privacy and Security Regulations**.

HIPAA Regulations

Module 1: HIPAA Privacy and Security Regulations

Module Introduction

The HIPAA Privacy Rule:

There are strict regulations regarding the use and disclosure of Protected Health Information (PHI).

To apply the Privacy Rule, you will learn:

- How and when to use and disclose PHI
- When patient authorization is required

The HIPAA Security Rule:

PHI should be reasonably safeguarded from intrusion or loss.

To apply the Security Rule you will learn:

- Ways to protect PHI
- Methods for destroying unneeded PHI

Module 1: HIPAA Privacy and Security Regulations

HIPAA Privacy Regulations

The HIPAA Privacy Rule

The Privacy Rule addresses the use and disclosure of health information as well as individuals' rights to understand and control how their health information is used.

A major goal of the Privacy Rule is to ensure that health information is properly protected while allowing that information to be used and disclosed as needed.

The Office of Regulatory Compliance (ORC) oversees HIPAA compliance for CU Denver and CU Anschutz. ORC provides policies that guide HIPAA compliance in all areas of campus operations.

You have an obligation to be sure that any PHI used or disclosed is done so using only the minimum necessary to accomplish the task.

Module 1: HIPAA Privacy and Security Regulations

HIPAA Privacy Regulations, continued

Protected Health Information (PHI)

The HIPAA Privacy Rule governs the protection of all individually identifiable health information held or transmitted by a **covered entity** or affiliates, in any form or medium (electronic, paper, or oral). The Privacy Rule calls this information **Protected Health Information** (**PHI**).

All patients have health information stored in physical and digital formats. Protected Health Information is any information that relates to:

- an individual's past, present or future physical or mental health or condition,
- the provision of health care to an individual, or
- the past, present, or future payment for the provision of health care to an individual.

Covered Entities

Covered entities are defined in the HIPAA regulations as (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which the US Department of Health and Human Services (HHS) has adopted standards.

Protected Health Information (PHI)

A thorough definition of PHI is as follows:

"Protected Health Information (PHI) is individually identifiable health information that is a subset of health information, including demographic information collected from an individual, and:

1. Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

    i. That identifies the individual; or
    ii. With respect to which there is a reasonable basis to believe the information can be used to identify the individual."

Module 1: HIPAA Privacy and Security Regulations

HIPAA Privacy Regulations, continued

Patient Authorization

In order to disclose PHI, you must have written authorization from the patient. The Office of Regulatory Compliance (ORC) has authorization forms for you to use on their Policies and Forms page (http://www.ucdenver.edu/research/ORC/HIPAA/Pages/policies.aspx).

Each authorization is only valid for the disclosures specified in the authorization. Even if the patient already has a signed authorization on file, new patient authorization must be obtained for any new disclosures of PHI.

Exceptions

There are exceptions. PHI can be used or disclosed for the purposes of **T**reatment, **P**ayment for care, or health care **O**perations (TPO) without written authorization from the patient.

Patient authorization is not required in the following cases:

- Disclosure to a health care provider for treatment purposes.
- Disclosure to the patient who is the subject of the information (or to a representative if the patient is a minor or incapacitated).
- Use or disclosure required for compliance with the HIPAA Administrative Simplification Rules.
- Disclosure to the US Department of Health and Human Services (HHS) when required for law enforcement purposes.
- Use or disclosure required by other law.

NOTE

Never access PHI unless it is necessary to perform your job duties, even your own information, or that of your friends, family members, and colleagues.

Module 1: HIPAA Privacy and Security Regulations

HIPAA Privacy Regulations, continued

Under HIPAA, patients have the right to:

- Request restrictions of the uses and disclosures of their PHI
- Request copies of their PHI
- Inspect their PHI
- Request amendments to their PHI
- Obtain a list of disclosures of their PHI
- Receive a notice of privacy practices

Health care providers should comply with any reasonable patient request for PHI, but may deny the request under certain circumstances. For example, health care providers do not have to provide an accounting of disclosures to patients when PHI was used or disclosed for TPO, and patients may not inspect their psychotherapy notes unless approved by the originator of the notes.

Module 1: HIPAA Privacy and Security Regulations

HIPAA Security Regulations

Covered entities have a responsibility to ensure the confidentiality, integrity, and availability of PHI they create, receive, maintain or transmit.

The Office of Information Technology (OIT) oversees HIPAA security compliance, with cooperation from ORC. OIT fulfills the university's obligation under HIPAA to identify potential security threats and make reasonable attempts to protect against them.

Individuals also have an obligation to be aware of technological safeguards to protect PHI from an end-user's perspective, and to take reasonable measures to act on those safeguards.

Module 1: HIPAA Privacy and Security Regulations

Conclusion

In this module, you saw that CU Denver and CU Anschutz have an obligation under HIPAA to protect the privacy and security of Protected Health Information (PHI).

The Office of Regulatory Compliance (ORC) and the Office of Information Technology (OIT), make and implement campus HIPAA policies. Both ORC and OIT are there to help you, as well, with any HIPAA-related policy or security questions you have.

For help with HIPAA-related questions, you can call one of the following numbers:

- For HIPAA Privacy matters: 303-724-1010
- For HIPAA Security matters: 303-724-4357

You also saw, briefly that individuals are responsible for safeguarding PHI. In the next module, you will learn methods of safeguarding PHI.

Continue to Module 2: Safeguarding PHI.

HIPAA Regulations

Module 2: Safeguarding PHI

Module Introduction

Protected health information (PHI) should be reasonably safeguarded from intrusion or loss.

This module will cover various types of PHI and reasonable safeguards you can implement to protect PHI.

This module will cover:

- Verbal communication
- Fax and telecommunications
- Social media
- Workspace safeguards
- Badge access

Module 2: Safeguarding PHI

Verbal Communication

Pay attention to your surroundings when discussing PHI with patients or coworkers. Ask yourself: is it possible for someone else to overhear this conversation? If it is, move the conversation to another location.

This is true whether your communication is in person or over the phone. Take a look around you, and if you are not alone, take it somewhere else.

HIPAA Regulations

Module 2: Safeguarding PHI

Social Media and HIPAA

Social media, blogs, YouTube and other ways we share our lives online open up new means of communicating with colleagues and sharing medical information. However, they also create privacy concerns on an unprecedented level.

Think before you post

When using social media:

- Always assume anything you put online is public, regardless of your privacy settings.
- Always assume anything you put online is stored on a server indefinitely and can be found, even if you delete it.

HIPAA Regulations

Module 2: Safeguarding PHI

Social Media and HIPAA

HIPAA violations online are taken seriously.

Example 1: Sharing too much on Facebook

The social media site Facebook had become more than just a way for staff at Innovis Health to catch up with friends.

In November 2008, nurses at the Fargo, ND–based healthcare system began using Facebook to provide unauthorized shift change updates to their co-workers. What once would have been a conversation became an update on their personal Facebook pages.

It was a convenient tool, because the nurses had “friended” each other through Facebook and thus could quickly read what each other wrote on their pages. They did not use patient names, but they did post enough specifics about patients so that the incoming nurses could prepare for their shift.

The problem was that everyone else “friended” to their Facebook pages could also read the information…

Becky Kirsch, RHIT, CCS, the director of health information management and privacy officer at Innovis Health (says:) “We needed to remind staff that that was certainly a HIPAA violation. Even if you don’t use patient names, [someone else] can still put two and two together.”

Social Media and HIPAA

Example 2: Patients can be identified, even without using standard identifiers

An ED physician in Rhode Island was fired, lost her hospital medical staff privileges, and was reprimanded by the Rhode Island Board of Medical Licensure and Discipline for posting information about a trauma patient on her personal Facebook page.

According to the Rhode Island Board of Medical Licensure and Discipline, "[She] did not use patient names and had no intention to reveal any confidential patient information. However, because of the nature of one person's injury … the patient was identified by unauthorized third parties. As soon as it was brought to [her] attention that this had occurred, [she] deleted her Facebook account." Despite the physician leaving out all information she thought might make the patient identifiable, she apparently did not omit enough.

From: How to Avoid Data Breaches, HIPAA Violations When Posting Patients' Protected Health Information Online

Retrieved from http://www.the-hospitalist.org/article/how-to-avoid-data-breaches-hipaa-violations-when-posting-patients-protected-health-information-online/?singlepage=1 on January 6, 2016

Social Media and HIPAA

Example 3: Unprofessional behavior online

An OB-GYN in St. Louis took to Facebook to complain about her frustration with a patient: “So I have a patient who has chosen to either no-show or be late (sometimes hours) for all of her prenatal visits, ultrasounds, and NSTs. She is now 3 hours late for her induction. May I show up late to her delivery?” Another physician then commented on this post: “If it’s elective, it’d be canceled!” The OB-GYN at issue then responded: “Here is the explanation why I have put up with it/not cancelled induction: prior stillbirth.”

Although the OB-GYN did not reveal the patient’s name, controversy erupted after someone posted a screenshot of the post and response comments to the hospital’s Facebook page. The hospital issued a statement indicating that its privacy compliance staff did not find the posting to be a breach of privacy, but the hospital added it would use this opportunity to educate its staff about the appropriate use of social media.

From: How to Avoid Data Breaches, HIPAA Violations When Posting Patients’ Protected Health Information Online

Retrieved from http://www.the-hospitalist.org/article/how-to-avoid-data-breaches-hipaa-violations-when-posting-patients-protected-health-information-online/?singlepage=1 on January 6, 2016

Social Media and HIPAA

Example 4: Results for All to See

An OB/GYN practice client ran into trouble when its receptionist recognized a woman from her neighborhood who came in for STD testing. The receptionist promptly posted a gleeful message on Facebook regarding the patient's medical issue after tracking down the test results, and common acquaintances on Facebook became privy to this confidential information. Improper access to patient information by office staff and dissemination of these details using social media are significant challenges that must be addressed.

Retrieved from: http://www.physicianspractice.com/blog/oops-you%E2%80%99re-violating-hipaa-and-didn%E2%80%99t-even-know-it on April 1, 2016.

Module 2: Safeguarding PHI

Social Media and HIPAA

Photographs are a form of PHI. It is possible to identify a patient from their image, in whole or in part. Do not take pictures of patients, unless you use the university's photographic equipment, and only take pictures for official business, not personal reasons.

Be aware of the background of your personal photographs and selfies, as well. You may intend only to take a picture of yourself, your coworkers, or the space around you, but be careful not to take pictures of patients or anyone else who may not want to be in that picture.

Who is in that selfie with you?

Module 2: Safegarding PHI

Workspace Safeguards

Before leaving your work area, be sure you have your badge with you. Any portable items that may have HIPAA data stored on them must be locked up or taken with you every time you leave your work area. This may include papers, USB drives, tablets, laptops, cell phones, external hard drives, CDs, DVDs, and any other small devices.

Module 2: Safeguarding PHI

Badge Access

Never share your access badge with anyone for any reason. If someone is following you into the secure area, don't hold the door open for them. Let them use their own badge for access.

Do not let people into secure areas if you aren't sure that they should have access. Turn and face them and tell them directly that they should use their own badge or seek assistance from campus security to get access if needed.

HIPAA Regulations

Module 2: Safeguarding PHI

Conclusion

The **Health Insurance Portability and Accountability Act** (**HIPAA**), is a US law that establishes privacy standards to protect patients' medical records and other health information. HIPAA exists to protect people's private information.

This course covered:

- The HIPAA Privacy and Security Rules
- How and when to use or disclose PHI
- Obtaining authorizations
- Ways to protect PHI, including:
    - Verbal communication
    - Social media
    - Workspace safeguards
    - Badge access

You are responsible for violations you commit. Ignorance of HIPAA regulations is not a valid excuse.

There is a 5-question quiz after this course. You must pass the quiz with at least 4 correct answers (80%) to receive credit.

Continue to **Contact Information**.

HIPAA Regulations

Contact Information

Office of Regulatory Compliance (ORC)
HIPAA Privacy Official: 303-724-1010
HIPAA Security Official: 303-724-0425
Signatory Official for Business Associate Agreements and Data Use Agreements : 303-724-1010

Office of Information Technology (OIT)
The OIT Help Desk Phone Number is: (303) 724-4357 (4-HELP from any campus phone)
The OIT Help Desk Email Address is: ucd-oit-helpdesk@ucdenver.edu

EthicsPoint
Anonymously report violations of law or violations of policy.
1-800-677-5590 or www.EthicsPoint.com.

Continue to **Resources**.

HIPAA Regulations

Resources

HIPAA information from HHS.gov

http://www.hhs.gov/hipaa/index.html

Office of Regulatory Compliance HIPAA policies and forms

http://www.ucdenver.edu/research/ORC/HIPAA/Pages/policies.aspx

Office of Information Technology Network and Security information

http://www.ucdenver.edu/about/departments/ITS/NetworkSecurity/Pages/default.aspx

Continue to the **Quiz**

HIPAA Regulations

Final Quiz

You must complete the final quiz with a score of 80% or better to receive credit for this course.

1. What does HIPAA stand for?
   - ◯ Health Information Privacy Advancement Act
   - ◯ Health Insurance Portability and Accountability Act
   - ◯ Heart Infarction Prevention and Avoidance Act
   - ◯ Hospital Intake Patient Access Act

2. Your coworker, Bob, forgot to bring his access badge to work again. If Bob is trying to enter a secure area behind you, what should you do?
   - ◯ Lend your badge to Bob.
   - ◯ Hold a door to the secure area open for Bob.
   - ◯ Tell Bob that he can prop the door open if he is only leaving for a minute.
   - ◯ Tell Bob to ask campus security for access.

3. What protected health information can patients have access to in their own records?
   - ◯ Patients can have access to all of their PHI at any time.
   - ◯ Patients can have access to only information directly related to payment.
   - ◯ Patients can have access to any information except psychotherapy notes, unless the psychotherapy notes have been approved for release by the provider.
   - ◯ Patients can only have access to information that has been approved in writing by their doctor.

4. When posting to personal or professional blogs or social media sites, remember that:
   - ◯ PHI posted on blogs and social media is not covered by HIPAA.
   - ◯ Anything you post should be considered public, regardless of privacy settings.
   - ◯ Pictures and selfies with patients in them are fine, as long as you only share them with friends and coworkers.
   - ◯ It is acceptable to share PHI on social media, as long as it is only intended for colleagues or the patient in question to see.

5. Amy is leaving her workspace for less than ten minutes. She takes her badge with her. However, there are papers and a USB drive containing PHI. What should Amy do with the papers and the USB drive?
   - ◯ Hide them under or behind other things where they are unlikely to be found, knowing that she'll be back soon.
   - ◯ Leave them, but only if there is a security camera guarding the area.
   - ◯ Lock them up, either in a dedicated lockable drawer or lock the office so unauthorized people can't get in.
   - ◯ Leave them. No one is likely to see or take anything, especially in a short period of time.

Submit by Email