

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Contents

- Health Insurance Portability and Accountability Act of 1996 (HIPAA) 1
- Welcome to HIPAA Awareness Training Content 3
 - HIPAA Awareness Training Outcomes 3
 - Why are we making a big deal out of HIPAA? 3
 - What is HIPAA? 3
 - Know Your HIPAA Acronym 4
 - HIPAA Legislation 4
 - How Do YOU Benefit from HIPAA? 4
 - Why do we have to comply?..... 4
 - Protected Health Information (PHI)..... 5
 - What is Individually Identifiable Health Information (IIHI)? 5
 - What is HIPAA Privacy? 5
 - The HIPAA Privacy Rule says... 5
 - Good privacy practices to remember... 6
 - More privacy practices to keep in mind..... 6
 - 2 Examples of Good Privacy Practice 6
 - Example #1 6
 - Example #2 6
 - Wrongful Disclosure of PHI 7
 - Two Scenarios Involving Privacy 7
 - Privacy Scenario #1 7
 - Privacy Scenario #2 8
 - Minimum Necessary 8
 - 3 Scenarios Involving “Minimum Necessary” 8
 - Scenario #1 8
 - Scenario #2 8
 - Scenario #3 9

What is Notice of Privacy Practices? 9

Notice of Privacy Practices Facts..... 9

Notice of Privacy – 3 True/False Questions 10

What are Potential Consequences of Violating HIPAA? 10

Penalties for Non-Compliance 10

3 Non-Compliance Scenarios 11

 Scenario #1..... 11

 Scenario #2..... 11

 Scenario #3..... 12

Additional HIPAA Training..... 12

HIPAA Updates 12

Confidentiality Agreement..... 12

Welcome to HIPAA Awareness Training Content

The following content was developed by a team of Trainers and Legal Advisors.

Disclaimer: These HIPAA Awareness Training materials are provided for the convenience of agencies of the State of Kansas and DCF. The information provided is for general educational and informational purposes only and is not intended to be or perceived to be legal advice. DCF does not make any representations whatsoever as to the accuracy or completeness of the information contained in these training materials. DCF does not make any guarantee that completion of this material ensures compliance with HIPAA training requirements. Users of these materials should consult with their own attorneys who are familiar with federal and state health laws to respond to specific questions or provide legal interpretations.

HIPAA Awareness Training Outcomes

To identify:

1. the components of HIPAA
2. how HIPAA affects a covered entity
3. appropriate actions to ensure privacy of Protected Health Information (PHI)
4. consequences for noncompliance with HIPAA

Why are we making a big deal out of HIPAA?

It's the law.

All staff must complete HIPAA Awareness Training to ensure compliance with HIPAA regulations regarding the privacy and security of protected health information (PHI).

What is HIPAA?

It's the Kennedy-Kassebaum Bill, also known as the Health Insurance Portability and Accountability Act of 1996, or HIPAA for short.

This law was enacted to help protect your rights to health insurance when you change jobs (Portability).

HIPAA also established new requirements to safeguard the privacy and security of personal health information (Accountability).

Know Your HIPAA Acronym

H is for Health

I is for Insurance

P is for Portability

A is for Accountability

A is for Act

HIPAA Legislation

HIPAA covers a broad range of issues.

HIPAA was established in 1996 with portability going into effect in 1997.

Accountability involves “Administrative Simplification” under which fall:

- Privacy
- Security
- Uniform Transaction, Code Sets and Identifiers

All these are elements of the HIPAA Legislation.

This training will address the Privacy element only.

How Do YOU Benefit from HIPAA?

- You are better able to continue health care coverage for existing conditions when you change jobs.
- The efficiency of the health care delivery system improves.
- HIPAA safeguards the privacy of your health care information.

Why do we have to comply?

We must comply because we are a Covered Entity (CE).

- Covered entities include:
 - Health Plans
 - Health Care Clearinghouses
 - Health Care Providers (who transmit any health information in electronic form in connection with a transaction covered by HIPAA)

Protected Health Information (PHI)

PHI is the key term to remember in guarding the privacy of individually identifiable health information (IIHI) in our day- to-day business practices.

PHI is . . .

- individually identifiable health information (IIHI)
- oral or written (paper or electronic)
- created or received by a covered entity
- relates to past, present or future health care or payments

What is Individually Identifiable Health Information (IIHI)?

IIHI is any information that connects health data to a specific person including such facts as:

- name
- birth date
- social security number
- health insurance ID number
- medical record number

What is HIPAA Privacy?

This part of the law prohibits the disclosure of Protected Health Information (PHI) in any form except as required or permitted by law.

The HIPAA Privacy rule mandates how PHI may be used and disclosed.

The Privacy Rule protects PHI in any form including but not limited to:

- e-mail
- fax
- information on the computer
- voice
- paper

The HIPAA Privacy Rule says...

- don't listen
- don't tell
- don't show

...any client's Protected Health Information (PHI) to anyone who does not have a legitimate right to see or hear that information.

Good privacy practices to remember...

Do put papers with PHI in a secured area.

Don't leave PHI exposed where other can see the content.

Do discuss particular cases in private.

Don't discuss a case in a public area where other people can overhear you.

More privacy practices to keep in mind...

Use passwords to keep other people from accessing your computer files.

Make sure your computer is locked when you leave your desk.

Minimize PHI in e-mails. Include as little as possible.

Protect fax machines that will be receiving PHI by putting them in secure and private locations.

2 Examples of Good Privacy Practice

Example #1

Jamila is entering data from her handwritten notes into a case file online.

Before she leaves for lunch, she places her handwritten notes inside the client's paper file, then locks the file in a cabinet.

Example #2

Two doctors are discussing a case in front of a nurse's station.

One of them notices another patient's family approaching, so he suggests they move the discussion to a more private location.

Wrongful Disclosure of PHI

If you observe someone wrongfully disclosing PHI...

1. First, talk to the person who is disclosing PHI. Tell them what you heard or saw and why you believe PHI has been wrongfully disclosed.
2. Then talk with your supervisor about the situation immediately.

If you wrongfully disclose PHI...

1. Write down...
 - whose PHI was disclosed
 - how it was disclosed
 - to whom
 - what day and time
 - and what was done to correct the problem
3. Then inform your supervisor immediately.

Two Scenarios Involving Privacy

Identify correct actions to be taken to protect PHI in the following scenarios.

Privacy Scenario #1

Two staff are discussing a case in a public area...

- The case involves medical coverage and eligibility concerns.
- There are many people nearby.

What should they do?

One of the following three answers is correct.

- Ask one of the people nearby for an opinion on the case being discussed.
- Stop talking about the case and move to a private location where their discussion cannot be overheard.
- Announce that they are talking about private information that contains PHI and so they shouldn't listen.

The correct answer is:

1. Move the discussion to a private location where it cannot be overheard.

Privacy Scenario #2

A custodian cleaning a conference room notices papers left out and unattended on one of the tables...

Since work in this building often involves PHI, what should the custodian do?

One of the following 3 answers is correct:

- Read the papers to see if they are confidential.
- Ignore the papers and continue working.
- Inform his supervisor that possible PHI is left on a table in an area he is assigned to clean.

The correct answer is:

3. Inform his supervisor.

Minimum Necessary

The term "minimum necessary" means...

- You must not share or obtain more PHI about a client than needed to do your job.
- HIPAA should not interfere with your ability to get information you need to do your job.
- ALL employees must avoid accessing information they don't need for their job.

3 Scenarios Involving “Minimum Necessary”

Scenario #1

Your team posted client information on a whiteboard in a room used regularly for other meetings and didn't erase it.

Is this okay?

The answer is no. Other people who don't need that information to do their jobs would see it. Always be sure you have not left any information behind.

Scenario #2

You are sent a list of clients who have been determined to be Medicaid eligible and will be receiving services at your agency that day.

As you look at the list, you see names of clients not assigned to you.

Should you have all this information?

The answer is no. You should only have access to information about your assigned clients.

Scenario #3

You are painting an office and see a client's closed file on the desk.

You notice the name on the folder tab is the same name of one of your friends.

You know you don't need to look at the file to do your job, so you leave the file unopened.

Did you do the right thing?

Yes. All employees should avoid access to health information they do not need to do their job.

What is Notice of Privacy Practices?

A written statement describing how medical information (PHI) may be used, disclosed, and accessed.

It also describes how your organization, as a covered entity, may use and disclose protected health information (PHI) to carry out treatment, payment, or health care operations (TPO) and for other purposes required or permitted by law.

All customers will receive a Notice of Privacy Practices to inform them of their individual rights.

Contact your appointed HIPAA Compliance Officer for a copy of your Notice of Privacy Practices and related policies and procedures.

Notice of Privacy Practices Facts

The only personal information the Notice of Privacy Practices is concerned with is PHI.

Individuals are given notice that we, as a covered entity, will share PHI for purposes of treatment, payment, and health care operations (TPO).

Individuals have a right to request that their personal information be amended or corrected.

We, as a covered entity, can give health related information to other agencies, including law enforcement, without the specific approval of the individual.

The Notice of Privacy Practices informs an individual of their right to file a complaint.

Notice of Privacy – 3 True/False Questions

True or False?

- The only personal information a Notice of Privacy Practices is concerned with is Protected Health Information (PHI).
- We, as a covered entity, may share health information when it is needed for treatment, payment and operations.
- We, as a covered entity, can give health related information to law enforcement agencies without the specific approval of the person.

All statements are true.

What are Potential Consequences of Violating HIPAA?

If a covered entity's employees and/or volunteers do not follow the rules set out by HIPAA, the Federal Government has the right to:

- Conduct an investigation
- Impose fines and/or jail sentences if found guilty

Stop and think before you act!

Penalties for Non-Compliance

Unintentional violations may result in:

- \$100 fine per violation
- up to \$25,000 for multiple violations of the same standard in a calendar year

Knowingly making unauthorized disclosure of PHI may result in:

- a \$50,000 fine
- imprisonment of not more than one year
- or both

Offenses which include false pretenses may result in:

- a \$100,000 fine,
- imprisonment of not more than 5 years
- or both

An offense with intent to sell information may result in:

- a \$250,000 fine
- imprisonment of not more than 10 years
- or both

3 Non-Compliance Scenarios

Scenario #1

Hunter is 21 years old and receives medical assistance because he has AIDS. Adrian works at a local insurance agency in the billing department. At lunch one day, Adrian told a coworker who has no involvement with the case that Hunter has AIDS.

Select the correct penalty for this violation from the 4 choices below.

- \$100 fine per violation, up to \$25,000 for multiple violations of the same standard in a calendar year for unintentional offenses.
- \$50,000 fine, imprisonment of not more than one year, or both for knowingly making an unauthorized disclosure of PHI.
- \$100,000 fine, imprisonment of not more than 5 years, or both for offenses which include false pretenses.
- \$250,000 fine, imprisonment of not more than 10 years, or both for an offense with intent to sell information.

Answer: 2. \$50,000 fine, imprisonment of not more than one year, or both, for knowingly making an unauthorized disclosure of PHI. Adrian made a deliberate disclosure of PHI.

Scenario #2

Phillip started faxing Kyle Conway's school and medical records to Kyle's foster care provider. He left the files unattended in the fax machine where others could see them.

Select the correct violation from the 4 choices below:

- \$100 fine per violation, up to \$25,000 for multiple violations of the same standard in a calendar year for unintentional offenses.
- \$50,000 fine, imprisonment of not more than one year, or both for knowingly making an unauthorized disclosure of PHI.
- \$100,000 fine, imprisonment of not more than 5 years, or both for offenses which include false pretenses.
- \$250,000 fine, imprisonment of not more than 10 years, or both for an offense with intent to sell information.

Answer: 1. \$100 fine per violation, up to \$25,000 for multiple violations of the same standard in a calendar year for unintentional offenses. This was an unintentional disclosure of PHI.

Scenario #3

Larry is running for political office. Lisa learned from her previous employment that Larry received treatment for a mental disorder. Lisa sold this information to a local newspaper.

Select the correct violation from the 4 choices below.

- \$100 fine per violation, up to \$25,000 for multiple violations of the same standard in a calendar year for unintentional offenses.
- \$50,000 fine, imprisonment of not more than one year, or both for knowingly making an unauthorized disclosure of PHI.
- \$100,000 fine, imprisonment of not more than 5 years, or both for offenses which include false pretenses.
- \$250,000 fine, imprisonment of not more than 10 years, or both for an offense with intent to sell information.

Answer: 4. \$250,000 fine, imprisonment of not more than 10 years, or both for an offense with intent to sell information. PHI was disclosed for money.

Additional HIPAA Training

Additional HIPAA training may be needed depending on your job.

HIPAA Updates

Updates will be provided if there are material changes in policy or HIPAA law.

Confidentiality Agreement

Please contact your HIPAA Compliance Officer and request a copy of your company's Confidentiality Agreement.