



HIPAA TRAINING

Commission on Dental Accreditation

© 2010 American Dental Association

Use of these materials by workforce members of the Commission on Dental Accreditation and the American Dental Association is permitted. Any other use, duplication or distribution by any other party requires the prior written approval of the American Dental Association.

CODA[★]
Commission on Dental Accreditation

What is HIPAA?

HIPAA is the federal law that governs the way “Covered Entities” handle the privacy and security of patients’ protected health information (PHI). HIPAA Covered Entities include health care providers and health plans that send certain information electronically.



Commission on Dental Accreditation

Why does a “Business Associate” need to comply with HIPAA?

- CODA may be deemed a “Business Associate” of certain institutions that are HIPAA Covered Entities.
- A Business Associate is an individual or entity that performs a function or activity on behalf of a HIPAA Covered Entity involving the use or disclosure of individually identifiable health information.
- Starting in 2010, Business Associates must comply with certain HIPAA Security and Privacy rules and implement training programs.



CODA HIPAA Training

- This HIPAA training program is designed to instruct you about your responsibilities when you have access to protected health information, or “PHI.”
- This training program will also help you understand how to respond to certain situations that might arise in the course of your work for CODA.



What is PHI?

Protected Health Information (PHI) includes:

1. Health information about an individual in any form, including electronic, hard copy (such as paper or films), and even oral information,
2. That was created or received by a health care provider health plan, or employer,
3. And that identifies the individual or that can be used to identify the individual.



Commission on Dental Accreditation

“ePHI”

- PHI in electronic form is sometimes referred to as “ePHI.”
- ePHI can include patient information in an e-mail, on FileWeb or SiteScape, or stored on a CD or a memory stick.

Is this PHI?

- A patient's dental chart with the patient's name, address, and telephone number.

Yes, it is PHI.

- A patient's dental chart with the patient's name, address, and telephone number is PHI because:
 1. It is health information about an individual
 2. It was created by a health care provider, and
 3. It identifies the individual.

Is this PHI?

- A patient's dental chart that does not have the patient's name or contact information, but that does have a patient number. You have access to a list of patient numbers with corresponding patient names.

Yes, it is PHI.

- The patient's dental chart and access to the key is PHI because it is:
 1. Health information about an individual
 2. Created by a health care provider, and
 3. It *can be used* to identify the individual.

When is patient information **NOT PHI?**

- When it is “de-identified.”
 - To “de-identify” PHI, all 19 “identifiers” have to be removed.

The 19 HIPAA Identifiers

1. Names
2. Locations, including addresses, cities, counties precincts, and zip codes
3. Dates (except year), including birth date, admission date, discharge date, and date of death, and all ages over 89 (or information that would indicate a date over 89)

The 19 HIPAA Identifiers

4. Telephone numbers
5. Fax numbers
6. E-mail addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers

The 19 HIPAA Identifiers

10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers,
including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers

The 19 HIPAA Identifiers

16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code (unless the key is not disclosed), and
19. Any other unique identifying number, characteristic, or code

The 19 HIPAA Identifiers

- In addition to removing the 19 identifiers, there must be no actual knowledge that the information could be used to identify an individual.

HIPAA Quiz

- On a site visit, you receive a patient chart that does not contain a name, treatment date, or any of the other 19 identifiers. Can information in this chart be disclosed?

Maybe.

- If all 19 identifiers are removed, and you have no actual knowledge that the information could be used alone or in combination with other information to identify an individual who is the subject of the information, it is de-identified and can be disclosed.
- But keep in mind that if information in the chart itself (like a unique dental condition) can be used to identify the patient, it constitutes PHI.

Avoid using “redaction” to de-identify PHI

- “Redaction” (for example, using a black marker to cover up the identifiers) should be avoided as a means of de-identifying PHI because redaction cannot be used to “secure” PHI under the Breach Notification Rule.

Avoid using “redaction” to de-identify PHI

- If redaction is the only available method (for example, for de-identifying a photo or radiograph), make sure the redaction is sufficiently thorough that the result would not pose a significant risk of financial, reputational, or other harm to the individual.
- Otherwise, disclosure may constitute a “breach” under the Breach Notification Rule.

What are the penalties for a HIPAA violation?

- The federal government imposes strict penalties on individuals and entities that violate HIPAA.
- Civil monetary penalties can range from \$100 to over \$50,000 for *each* HIPAA violation.
- A knowing and wrongful disclosure of PHI can also result in criminal penalties that include fines and imprisonment.

HIPAA Quiz


- On a site visit at an orthodontic program, you pass a young man in the reception room who is waiting for his appointment. He looks familiar, and a few minutes later you realize that he is a well-known actor who is a student in the university's drama program.
- Can you tell your daughter, who is a fan, that you saw him in the reception room?

You should not disclose this information.

- The fact that the young actor is an orthodontic patient is PHI. Although seeing him in the waiting room may be an “incidental exposure,” HIPAA Privacy requires Business Associates like CODA to reasonably safeguard protected health information to limit incidental uses or disclosures.

HIPAA Quiz

- During a site visit at a dental school, you are given access to the dental chart of a patient who was treated at the school. You notice that the patient has oral cancer. You are a specialist in the treatment of oral cancer and you are involved in several research studies. Can you note the patient's name and contact information and contact her?



No, that would be a disclosure of PHI in violation of HIPAA.

- The patient's name and contact information and the fact that she has oral cancer is PHI. You may not contact her or disclose the PHI to your practice.
- In addition, HIPAA has strict rules about using PHI for marketing purposes.

CODA HIPAA Compliance

- CODA's HIPAA **Security Official:**

Dr. Anthony Ziebert

Director

Commission on Dental Accreditation

312-440-4653

CODA*

Commission on Dental Accreditation

CODA HIPAA Compliance

- CODA's Backup HIPAA Security Official:

Dr. Laura M. Neumann

Senior Vice President

Education/Professional Affairs

Division of Education

312-440-4653

CODA*

Commission on Dental Accreditation

The CODA Training Manual

- Refer to the current CODA Training Manual. It contains detailed procedures and requirements that CODA employees and volunteers must follow.
- The following slides contain **examples** of the procedures and requirements in the Training Manual.

Training Manual Examples: CODA HIPAA Compliance

- All CODA employees and volunteers must follow the CODA HIPAA Compliance Policies and Procedures and Training Manual
- CODA will provide a copy of these documents to CODA employees and volunteers. Additional copies are available on FileWeb and from CODA.





Training Manual Examples: Documentation

- Ask the Security Official for any HIPAA documentation you require
- Give any HIPAA documentation you receive or create to the Security Official

Training Manual Examples: HIPAA Compliance Inside CODA

- Comply with facility security rules
- All visitors must be supervised
- Hard copy PHI must be stored in locked files

Training Manual Examples: HIPAA Compliance Outside CODA

- Never leave a laptop unattended that is not secured with a cable lock according to manufacturer's instructions
- Log off or lock your session before leaving your computer unattended
- Set up a screensaver with an automatic password lock after 30 minutes of inactivity



Training Manual Examples: Passwords

- Never share, write down, or post passwords
- Protect your computer with a login password
- Choose a “strong” password (at least 8 characters long, a mix of upper and lower case letters, numbers and symbols, and a word that cannot be found in the dictionary)

Training Manual Examples: Laptop Security

- Store laptops locked and out of sight
- Never write down your password or store it on your laptop or in your laptop case
- Contact the police and the Security Official immediately if you lose your laptop

Training Manual Examples: Computer and Internet Use

- Never access electronic PHI using anything other than a desktop or laptop computer
- Never download or print PHI unless you are an ADA employee using an ADA computer
- Never access PHI using an Internet café or hotel business center

Training Manual Examples: Electronic Media

- Do not save PHI to removable media such as floppy disk, CD-ROM, or DVD-ROM
- Do not download PHI to an unencrypted portable storage device

Training Manual Examples: De-Acquisition

- Erase your hard drive using approved procedures before de-acquiring a computer
- Follow approved procedures to dispose of removable media (e.g., CD-ROM) and how to erase PHI from a storage device (USB drive, thumb drive, etc.)
- Erase PHI from removable media using approved procedures

Training Manual Examples: Report immediately to the Security Official

- Loss of PHI in any format
- A security incident or a breach of PHI
- A request from an individual or patient
- A suspected HIPAA violation
- Unauthorized use of or access to PHI

Training Manual Examples : De-Identifying PHI

- Always de-identify PHI before including it in a CODA site visit report or other document
- De-identify PHI by removing the 19 HIPAA identifiers
- Redaction should be avoided as a means of de-identifying PHI

Training Manual Examples: Access to PHI

- Each CODA employee and volunteer is authorized to access only the PHI necessary for his or her job or assignment
- CODA volunteers may not download or make copies of PHI
- Log disclosures of PHI (other than disclosures for accreditation purposes) and report them to the Security Official

Training Manual Examples: Destruction of PHI

- Secure PHI following the Breach Notification *Guidance*
- Used approved techniques when authorized to destroy hard copy PHI
- Used approved techniques when authorized to destroy electronic media

HIPAA Situation #1

- On a CODA Site Visit you notice some patient dental charts in a recycling bin on the sidewalk outside the building. What do you do?

Report the information **immediately** to the CODA Security Official

- You may have discovered a breach of unsecured PHI. As a Business Associate, CODA has a legal obligation to report the information to the Covered Entity within a set timeframe. Reporting immediately to the CODA Security Official allows CODA to fulfill its legal obligation under HIPAA.



HIPAA Situation #2

- On a CODA site visit you are given access to all of the institution's patient charts. Your stepson is a student at the university and you know he received treatment at the dental school. Can you access his chart if your purpose is to confirm that he received appropriate dental care?

No.

- A CODA Consultant must use the minimum necessary PHI to accomplish the purpose of disclosure, that is to say, his or her CODA responsibilities. Accessing the charts of individuals for any other purpose would violate the minimum necessary rule.

CODA*

Commission on Dental Accreditation

HIPAA Situation #3

- You are participating in a site visit at an institution that was recently involved in a scandal involving negative publicity. While you are leaving the building at the end of the day, a newspaper reporter asks you a question about the institution. What should you do?

Decline to speak to the press

- CODA Consultants are not authorized to speak to members of the media about their work, whether or not doing so would disclose PHI.
- Moreover, disclosing PHI to a reporter would violate HIPAA.

HIPAA Situation #4

- You and another CODA Consultant are seated together on an airplane flight after a site visit. The two of you would like to use the time to discuss the site visit and work on the site visit report. Is there a HIPAA issue?



Yes.

- Always take care not to discuss PHI in public.

Documentation of HIPAA Training

- CODA is required by law to maintain documentation that all CODA Consultants have received HIPAA training.