

# HIPAA TRAINING 2025

Commission on Dental Accreditation

# “HIPAA”

- The Health Insurance Portability and Accountability Act of 1996
- HIPAA:
  - Is a federal law
  - Applies to “covered entities” and their “business associates”
  - Regulates protected health information (“PHI”) (generally, patient information that identifies, or could be used to identify, an individual)

# Why does CODA need to comply with HIPAA?

- Some of the institutions that CODA accredits are HIPAA covered entities
- CODA may be deemed to be their business associate
- HIPAA business associates generally:
  - Provide a service that requires access to PHI
  - Are directly responsible for HIPAA compliance
  - Must have HIPAA policies & procedures, training, etc.

# When Might I Access PHI?

- CODA workforce members (volunteers and staff) are authorized to access PHI on site visits for accreditation purposes.
- Although CODA prohibits programs from providing PHI outside of site visits, and imposes penalties on programs that do so, from time to time a program may send PHI to CODA or CODA workforce members.

# Discovering PHI Offsite

- Immediately notify the Security Official if you come across identifiable patient information outside of a site visit.
- Examples include patient information in a self-study, an email, etc.
- HIPAA applies if even one of the 18 identifiers is there (such as treatment date or record number), even if patient name, address, etc. are removed.

# Safeguards Overview:

- Here are some important safeguards:
  - Access PHI onsite only
  - Do not make or retain PHI or copies
  - De-identify all patient info in reports
  - Read and adhere to all CODA training materials
  - Protect all sensitive information

# Safeguards Overview:

- Here are some important safeguards:
  - Use full disk encryption on any computer used for CODA work
  - Do not access CODA information on a device other than a desktop or laptop computer
  - Immediately report any PHI accessed offsite, suspected breaches, security incidents, violations

# Part 1

# Security Official

# CODA HIPAA Security Official:

- Security Official:  
Sherin Tooks, EdD, MS  
Director, Commission on Dental Accreditation  
312-440-2940
- Backup Security Official:  
Peggy Soeldner  
Manager, Advanced Dental Education  
312-440-2788

# CODA HIPAA Security Official:

- Contact the Security Official immediately if you:
  - Have questions about HIPAA compliance
  - Suspect a HIPAA violation or a violation of CODA HIPAA policies and procedures
  - Receive a complaint about CODA HIPAA compliance
  - Receive a request or document relating to HIPAA or PHI

## Part 2

# Protected Health Information (“PHI”)

# What is PHI?

- PHI is information, including demographic information:
  - about an individual's past, present or future:
    - physical or mental health
    - treatment, or
    - payment for health care
  - that identifies the individual, or could be used to identify the individual, and
  - that was created or received by a health care provider, health plan, employer or clearinghouse
  - in oral or recorded format (electronic or hard copy)
- ***When in doubt, treat health information as PHI***

# Hard Copy and Electronic PHI

- HIPAA protects PHI in all forms, such as oral/spoken information, paper documents, photographs, radiographs, and electronic data
- PHI in electronic form is sometimes referred to as “ePHI.” Examples of ePHI can include data in an e-mail, or ADA Connect, in CODA’s Electronic Portal, or stored on a CD or a USB drive.

## HIPAA Enforcement:

- Enforcement authority
- Civil penalties
- Criminal penalties
- Sanctions

# Who Enforces HIPAA?

- **HIPAA is enforced by the federal Office for Civil Rights (“OCR”), which is an agency of the U.S. Department of Health and Human Services (“HHS”)**
- **State attorneys general also have HIPAA enforcement authority**
- **Any individual can submit a HIPAA complaint to OCR or the state AG and trigger an investigation**

# Civil Penalties for HIPAA Violations

- **The government can impose substantial penalties on covered entities and business associates that violate HIPAA**
- **Depending on the violation, the penalties can amount to thousands, or even millions of dollars**

# Resolution Agreements

- **The government can also impose burdensome resolution agreements on covered entities and business associates that violate HIPAA**
- **For examples of HIPAA penalties, settlements, and resolution agreements, visit:**  
<https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html>

# HIPAA Criminal Enforcement

- The government can impose criminal penalties for HIPAA violations on individuals and entities that obtain, use or disclose PHI without authorization.

# Criminal Penalties

- Even looking at PHI without authorization can be a federal crime
- HIPAA criminal violations are punishable by substantial fines and/or imprisonment

# Do HIPAA Criminal Penalties Apply to Individuals?

- Yes. Congress has made it clear that criminal penalties apply to any person who obtains or discloses individually identifiable health information in violation of HIPAA, even if the person is not a covered entity or business associate or an employee of a covered entity or business associate.

# Why are HIPAA Penalties So Severe?

- Improper use and disclosure of PHI can result in:
  - Reputational harm (health information is private and often sensitive)
  - Financial identity theft (using another person's identity to purchase goods and services, obtain credit, etc. is a crime)
  - Medical identity theft (using another person's identity to obtain medical items and services is a crime)
- Identity theft is a fast-growing crime

# Sanctions

- HIPAA also requires CODA to apply sanctions to workforce members who violate HIPAA or CODA HIPAA policies and procedures. Sanctions may include private conversations to review safeguards, written reminders, mandatory additional training, oral or written warnings, or termination, as appropriate.

## HIPAA Compliance:

- CODA training materials
- Examples of compliance requirements

# HIPAA Training

- CODA is required to train all workforce members to comply with HIPAA. Examples of CODA HIPAA training materials include:
  - This PowerPoint
  - The CODA HIPAA Training Manual
  - The CODA HIPAA Policies & Procedures
  - Periodic “security reminders” from CODA

# CODA HIPAA Policies & Procedures

- Each workforce member is responsible for reading, understanding, and adhering to the provisions in the CODA HIPAA training materials
- The Security Official distributes these materials to all workforce members and post them on ADA Connect. Let the Security Official know if you need additional copies.

# Examples of HIPAA Compliance Requirements

- The next few slides give examples of some important HIPAA compliance requirements:
  - Permitted uses and disclosures of PHI
  - The minimum necessary rule
  - Incidental disclosures
  - Reporting security incidents
  - De-identifying PHI

# Permitted Uses and Disclosures of PHI

- With limited exceptions, CODA workforce members are only permitted to access, use and disclose PHI as necessary to carry out their accreditation responsibilities
- Report any other uses or disclosures immediately to the Security Official

# The “Minimum Necessary” Rule

- Always request, use, or disclose the minimum necessary PHI for the purpose of the request, use, or disclosure

# Minimize Incidental Disclosures

- Take reasonable precautions to limit “incidental” uses or disclosures
- An “incidental” use or disclosure is one made pursuant to an otherwise permitted or required use or disclosure (for example, if someone who is not authorized to access PHI overhears a permissible conversation between two dentists)
- Examples of “reasonable precautions:” don’t discuss PHI in public, don’t leave PHI visible on a computer screen if there is a visitor nearby

# Report Security Incidents Immediately

- A security incident involves electronic PHI, and occurs when there is an attempted or successful unauthorized:
  - access, use, disclosure, modification or destruction of information, or
  - interference with system operations

# Report Security Incidents Immediately

- Examples of security incidents:
  - Lost laptop, cell phone, or other electronic media or device
  - Lost CD-ROM or USB drive that contains PHI
  - Hacking, virus, or malware
  - Misdirected email containing PHI
- Report all security incidents and suspected security incidents immediately

# Report Security Incidents Immediately

- Report suspected “security incidents” immediately to the Security Official
- CODA may have certain legal obligations when a security incident is discovered

# Site Visit Reports Must Not Contain PHI That Has Not Been “De-Identified”

- To “de-identify” PHI, all 18 “identifiers” have to be removed, and CODA must not have actual knowledge that the information could be used, alone or in combination with other information, to identify an individual who is a subject of the information
- The 18 HIPAA “identifiers” are listed in the Training Manual

# Redaction

- “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
- Ask the Security Official for instructions if you need to de-identify PHI

# Individual's Rights Under HIPAA

- HIPAA gives individuals rights over their PHI. For example, individuals may request:
  - an accounting of disclosures of their PHI
  - an amendment to their PHI
  - access to their PHI (inspection or copies)
- These rights are subject to certain important limitations and conditions

# Refer Individuals' Requests to the Security Official

- If you receive a request from an individual that pertains to PHI:
  - Do not grant the request
  - Explain that the Security Official must handle all such requests
  - Notify the Security Official immediately

# Breach Notification

# The HIPAA Breach Notification Rule

- If there is a “breach” of “unsecured” PHI, HIPAA requires a business associate to provide notice to the covered entity without unreasonable delay. In no case may notice be provided later than 60 days after discovery of the breach.
- Electronic PHI is unsecured if it is not properly encrypted. Hard copy PHI (paper documents, photos) can only be secured through proper destruction.

# How Do Breaches Occur?

## Examples of potential breaches:

- Lost laptops and other electronic devices
- Unauthorized access to paper documents or electronic data
- Mail, fax or email sent to the wrong person
- PHI disclosed to an unauthorized person
- PHI posted online
- Improper disposal

# Cost of a Data Breach

- For patients, covered entities, and business associates, a data breach can:
  - Be very stressful, time-consuming and expensive
  - Result in financial and reputational harm

# Definition of a Breach

- Generally, a breach is:
  - unauthorized acquisition, access, use or disclosure of PHI
  - in violation of the Privacy Rule
  - that compromises the security or privacy of the PHI
- Immediately report all suspected breaches to the Security Official

# Breach Notification

- If the covered entity determines that the incident constitutes a breach of unsecured PHI, the covered entity must notify:
  - Affected individuals,
  - The federal Office for Civil Rights, and
  - In some cases, the media

# State Data Breach Laws

- In addition to HIPAA, state law may require notification if “sensitive personal information” (“SPI”) is breached, whether or not the SPI is “health information”
- In many states, SPI includes an individual’s name plus one or more of the following:
  - Social Security number
  - Credit or debit card number
  - Driver’s license number or state I.D. number
  - Account number information
- In some states, SPI may also include name plus medical information, health plan number, biometric identifiers such as fingerprint and retinal scan data, and other data elements

# SPI

- The definition of SPI varies from state to state. If you discover that any sensitive personal information has been disclosed to, or accessed by, an unauthorized individual, notify the Security Official immediately.

# Examples of SPI

- A statement containing an individual's name and credit card number
- A curriculum vitae containing an individual's name and Social Security number
- An statement or explanation of benefits (“EOB”) containing an individual's name and Social Security number (a document may be both PHI and SPI)

# Avoid Breaches

- To minimize the chances of a breach:
  - Comply with CODA HIPAA requirements
  - Encrypt electronic PHI to “secure” it (and protect the decryption key or password)
  - Properly de-identify patient information in reports
- Instructions for securing ePHI are in the Training Manual

# OCR HIPAA Breach Webpage

- The OCR website lists HIPAA breaches involving 500 or more individuals:

[https://ocrportal.hhs.gov/ocr/breach/breach\\_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf)

# Conclusion

# The CODA Training Materials

- Every CODA workforce member is responsible for understanding and complying with the instructions in the training materials. Please read them carefully and refer to them as needed. If you have a question that is not answered in these materials, contact the Security Official.

# Report immediately to the Security Official

- Any HIPAA-related questions
- Loss or suspected breach of PHI or SPI
- Suspected unauthorized access, hacking
- A request from an individual regarding PHI
- A suspected HIPAA violation
- Unauthorized use, disclosure or access
- Receipt of any HIPAA-related document

# Copyright

- © 2010-2025 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.

# Full Disk Encryption

Commission on Dental Accreditation

# What is Full Disk Encryption (FDE)?

- It is a security tool that unobtrusively encrypts your entire computer hard drive
- FDE secures all data stored on your hard drive automatically and transparently without any user interaction
- If your computer is lost or stolen, FDE can help avoid the possibility of a data breach as long as the password is not compromised

# What is Full Disk Encryption (FDE)?

- This encryption secures your hard drive so that no one can access it without a valid password
- The hard drive is encrypted, but the files on the hard drive are not encrypted. This means you can access and use the files without decrypting them first. (Files can still be individually encrypted if you wish.)

# I already use a password with my computer, isn't that enough?

- Unfortunately, no. Without FDE, your Windows or your Macintosh password can be bypassed
- If your computer is lost or stolen, it is easy for someone to access your data. They do not need your login password to do so
- Password protection alone does not stop a data breach

# What if I use a fingerprint or retinal scan?

- These alone do not stop a data breach. If the computer has sensitive information and is lost or stolen, breach notification may still be required under HIPAA and state law.

# How hard is it for an attacker to access data on a non-encrypted hard drive?

- It's very easy. All it takes is a bit of technical knowledge or some researching.
- One way is to boot another operating system from a USB drive.
- For example, a person with your computer can boot their own copy of Windows from a USB key.
- Once the attacker logs in, they would be able to read your data.

# How hard is it for an attacker to access data on a non-encrypted hard drive?

- Another way is to remove your hard drive from your computer and temporarily attach it to another computer using special adapter cables.
- In either case, if someone had possession of your computer, any file on your computer could be accessed without your permission or knowledge.
- Even if you get your lost computer back, there is no way to prove the data was not accessed when it was out of your possession

# Full Disk Encryption

- **If your computer is lost or stolen, the only way to be sure that whoever has your computer will not be able to access your files is to use “Full Disk Encryption” and protect the password**
- **CODA requires you to run “Full Disk Encryption” on the device you use to access CODA related materials**

# How does Full Disk Encryption work?

- During the installation process of the FDE software you will be prompted to create a password or a recovery key will be generated
- Make a note of this password or recovery key and store it in a secure location
- This key is used for the encryption and decryption process
- You will need it if there is ever a problem with your FDE

# How does Full Disk Encryption work?

- Some Full Disk Encryption software will allow you to create a pre-boot password and others will use your default login password.
- For example, if you are using a Mac and you enable File Vault. Once the setup is complete and you restart your Mac, you will use your account password to unlock your disk.

# Why is it important to use Full Disk Encryption?

- Programs have been instructed not to send sensitive information. But as we know, sometimes people forget.
- If your computer is lost or stolen, having Full Disk Encryption lets us confirm that “no sensitive data that might have been on that computer could be accessed.”

# Why is it important to use Full Disk Encryption?

- PHI protected by Full Disk Encryption is considered “secure” under the HIPAA Breach Notification Rule, as long as the Full Disk Encryption is FIPS 140-2 (Federal Information Processing Standards) validated and the password is not compromised. (more on FIPS 140-2 in a few slides)

# Why is it important to use Full Disk Encryption?

- If “secured” PHI is breached (e.g., through loss or theft of a laptop), the Breach Notification Rule does not require notification. In other words, the HIPAA Breach Notification Rule only requires notification where there is a breach of “unsecured” PHI. State data breach laws may also provide exceptions for encrypted sensitive data.

# Where can you obtain Full Disk Encryption?

- There are a number of appropriate products available, but here are a couple of options:
  - Microsoft BitLocker
  - Apple FileVault

# Where can you obtain Full Disk Encryption?

- Bitlocker is available on:
  - Windows 10 Pro
  - Windows 10 Enterprise
  - Windows 10 Education
  - Windows 8.1 Pro
  - Windows 8.1 Enterprise
- Windows 7 is no longer supported by Microsoft and should not be used for CODA work

# Where can you obtain Full Disk Encryption?

- FileVault is available on:
  - macOS Catalina
  - macOS Mojave
  - macOS High Sierra
  - macOS Sierra
  - OS X El Capitan
  - OS X Yosemite
  - OS X Mavericks
  - OS X Mountain Lion
  - OS X Lion

# Where can you obtain Full Disk Encryption?

- If you don't want to use one of the previously recommended products, be sure to use one that is FIPS 140-2 validated
- If your FDE product is not FIPS 140-2 validated, it may still be appropriate as long as it uses AES encryption with 128 bit keys or longer.
- If you have questions, please contact the CODA HIPAA Security Official.

# Where can you obtain Full Disk Encryption?

- Check with your organization's IT department or other technical resource to see if your laptop already has appropriate FDE enabled. You may not realize it is already running.

# Notifying the Security Official

- Do I need to notify the Security Official if I lose my FDA-protected computer and the password wasn't compromised? Yes. The Security Official will make a record of the report and circumstances to document HIPAA compliance and to establish why breach notification was not provided.

# Full Disk Encryption

## Final Notes

# Full Disk Encryption

- When you install Full Disk Encryption, be sure to be extra vigilant about doing regular backups.
- Be sure to encrypt your backups
- Remember to keep your FDE password or recovery key in a secure location.
- If you have a hard drive failure, it will be impossible to send your hard drive to a vendor to try to recover data files without the encryption password or recovery key.