

# Privacy and Data Security Summary: Site Visitor Responsibilities

(Rev. 11/16/2023)

Privacy and data security laws such as HIPAA may require CODA to take certain steps to protect sensitive data such as patient records and social security numbers. These steps may include training, developing written policies and procedures to protect sensitive data, and sending notice if CODA discovers a data breach. The following is a summary of some of the safeguards in CODA's HIPAA Compliance Policies and Procedures and the CODA Privacy and Data Security Training Manual. For full information, please refer to those documents.

- Protected health information (“PHI”) protected by HIPAA includes identifiable health information about an individual in any form, including electronic, hard copy (such as paper or films), and oral information, which identifies the individual or that can be used to identify the individual. Information identifies an individual if it contains one or more “patient identifier” (see attached list) or can otherwise be used to identify a patient.
- PHI in electronic form is sometimes referred to as “ePHI” and can include patient information in an e-mail, in SharePoint or ADA Connect, or stored on USB drive.
- Sensitive personal information (“SPI”) includes data such as social security numbers, credit and debit card numbers, passport numbers, driver’s license numbers or state ID numbers, or other government issued ID numbers that could be used to harm an individual if they fall into the wrong hands (see attached “Sensitive Information”).
- CODA volunteers (site visitors, review committee members, and Commissioners) and staff must comply with CODA’s HIPAA Compliance Policies and Procedures and CODA’s Privacy and Data Security Training Manual. Federal law requires CODA to train volunteers/staff and impose sanctions on those who do not comply with CODA’s HIPAA policies and procedures.
- Site Visitors are only authorized to access the PHI/SPI that is necessary for conducting the accreditation site visit.
- CODA volunteers may only access PHI/SPI on site during the time of a site visit.
- CODA volunteers may not download or make hard copies of PHI/SPI.
- CODA volunteers must not retain any program or CODA materials beyond their intended use to conduct work on behalf of CODA. (See Disposal of Program Documentation, below)
- Avoid unnecessary disclosures of PHI/SPI by keeping voices low when discussing PHI/SPI in public.
- Do not leave a computer that has been used to access PHI/SPI unattended without logging off.
- Set your computer to automatically lock if there is no activity for fifteen (15) minutes; enable screen saver locks so that you must use your username and password to unlock a locked system or device.
- Protect your laptop against loss or theft.
  - 1) Avoid leaving your laptop in a hotel room. If you must leave it in a hotel room, lock it inside an in-room safe or another piece of luggage.
  - 2) Never leave a laptop unattended unless it has been secured with a cable lock according to the manufacturer’s instructions. Be aware that a cable lock can be cut with a small bolt cutters, so do not depend on one if your computer will be left alone for a long time or in a place without a lot of other people around.
  - 3) At airport security, place your laptop on the conveyor belt only after the belongings of the person ahead of you have cleared the scanner. If you are delayed, keep your eye on the laptop until you can pick it up.
  - 4) Tape your business card to the underside of your electronic devices.

- 5) Avoid leaving your laptop in a parked car.
  - 6) Never store your computer password with the computer (for example, in your laptop case)
- If your computer is lost or stolen contact the police and call the CODA office **immediately** at 312-440-4653 (the CODA main office number).
  - Never access ePHI/SPI using anything other than a desktop or laptop computer (for example, do not use your smartphone, or similar device to access ADA Connect).
  - Do not access ePHI/SPI using a computer that is not under your control, such as the computers at Internet cafés, hotel business centers, and friends' homes.
  - Do not access ePHI/SPI (or access ADA Connect) from an untrusted Internet location (hotel Internet, coffee shop, neighbor's WiFi, etc.).
  - **Examples of things that you must report immediately to the Security Official:** Call the CODA main office number: 312-440-4653 immediately if you discover:
    - Any loss of any PHI/SPI in any format, including any laptop or other device that has been used to access or store PHI/SPI.
    - Any possible or suspected "breach" of PHI. A breach is generally defined as the unauthorized acquisition, access, use, or disclosure of PHI/SPI. Examples of possible breaches include:
      - throwing a CD containing PHI/SPI away in a wastebasket
      - losing a laptop that has been used to access PHI/SPI
      - showing ePHI/SPI to a colleague who is not authorized to access it
      - discussing PHI/SPI with a friend who is not authorized to access it
      - accidentally leaving a memory stick with unencrypted ePHI on a store counter
      - leaving a paper document containing PHI/SPI in the public area of an office
    - Any individual's request (such as a patient or patient's representative) to:
      - access PHI
      - amend PHI, or
      - for an accounting of disclosures of PHI
 Do not grant the request—tell the individual you must refer the request to the CODA office
    - Any request or communication from the U.S. Department of Health and Human Services, the Office for Civil Rights, or a state attorney general.
    - Any suspected violation of CODA's HIPAA Policies and Procedures or CODA's Privacy and Data Security Training Manual.
    - Any pattern of activity or practice of an institution or a downstream Business Associate (e.g., an ADA vendor or subcontractor) that appears to constitute a breach or violation of the entity's obligations concerning privacy or security.
    - Any misdirected e-mail U.S. mail, or courier delivery containing PHI/SPI.

**Disposal of Program Documentation:** Please remember that ALL program documentation, including the self-study, CDs, USBs, and E-mails from the Program and Commission MUST be securely disposed of after you have reviewed and approved the preliminary draft site visit report. You must not retain any program or CODA information beyond its intended use to conduct work on behalf of CODA.

To securely dispose of materials, you are requested to personally do the following:

- **"Securely Delete" files from your computer:**
  - Files downloaded from CODA's E-Portal may save to the "Downloads" folder on your computer as well as another location that you have chosen to save the document. You must securely delete files from all locations on your computer. To find the Downloads folder, click on "This PC" or equivalent icon, then click on "Downloads" folder. Follow instructions below for deletion of files on Windows or Mac devices.

- To securely delete a file if you are using Windows:
  - Click once on the file to highlight it but not open it
  - Click “shift” and “delete” to permanently delete the file
  - Check your Recycle Bin to ensure the file is permanently deleted. If it appears in the Recycle Bin, delete it again
- To securely delete a file if you are using a Mac:
  - Delete the file
  - Go to your Mac’s Finder menu (upper left-hand side of your screen)
  - Choose "Secure Empty Trash..."
- “Securely Delete” an email:
  - Click once on the email to highlight it but not open it
  - Click “shift” and “delete” to permanently delete the email
  - Check your Deleted Items Folder to ensure the email is permanently deleted. If it appears in the Deleted Items Folder, delete it again
- “Securely Delete” an attachment from your email:
  - Open the email
  - Click on the attachment to highlight it but not open it
  - Click “shift” and “delete” to permanently delete the attachment
  - Check your Deleted Items Folder to ensure the file is permanently deleted. If it appears in the Deleted Items Folder, delete it again
- Shred paper documents so that they cannot be read or reconstructed. If you use a document destruction firm to shred your documents:
  - Store documents in a securely locked bin prior to shredding
  - Confirm that a compliant business associate agreement is in place with the document destruction firm
  - Confirm that the firm destroys documents so that the documents cannot be read or otherwise reconstructed
  - Verify identity of the recycling firm representative as appropriate
- Shred CDs
- For data stored on external USB drives:
  - If the files containing Sensitive Information or Patient Identifiers are encrypted, or if the external USB drive is itself encrypted
    - Simply delete those files, following the instructions below titled “Securely Delete files from your computer”
  - If the files are not encrypted, or if the external USB drive is not encrypted, then you will need to securely wipe or securely dispose of the entire USB memory key, thumb drive or flash drive:
    - Use a utility, such as Disk Wipe (<http://www.diskwipe.org/>) to overwrite the entire storage space of the device.
      - NOTE: Disk Wipe only works for Windows. If you are working on a Mac, please contact CODA for further instructions.
    - If you can not use a utility to overwrite the USB drive, then you must destroy the USB memory key, thumb drive, or flash drive by smashing the components and circuit board using a heavy hammer (Please be sure to wear appropriate eye protection)
      - For USB drives that have moving parts, i.e. external hard drives, contact CODA for additional instructions

## Sensitive Information and Patient Identifiers

1. **Sensitive Information.** To protect the privacy of individuals and to comply with applicable law, the Commission on Dental Accreditation (“CODA” or “the Commission”) **prohibits all programs/institutions from disclosing in electronic or hard copy documents** provided to CODA other than during a site visit, any of the following information (“Sensitive Personal Information” or “SPI”):

- Social Security number
- Credit or debit card number or other information (e.g., expiration date, security code)
- Drivers’ license number, passport number, or other government issued ID
- Financial account number
- Health insurance information, such as policy number of subscriber I.D.
- Medical information, such as information about an individual’s condition, treatment, or payment for health care
- Mother’s maiden name
- Taxpayer ID number
- Full date of birth
- Any data protected by applicable law (e.g., HIPAA, state data security law)
- Biometric data, such as fingerprint or retina image
- Username or email address, in combination with a password or security question that permits access to an online account

2. **Patient Identifiers.** Before submitting information about a patient to CODA other than during a site visit, a program/institution **must remove the following data elements** of the individual, and of relatives, household members, and employers of the individual (the “Patient Identifiers”):

1. Names, including initials
2. Address (including city, zip code, county, precinct)
3. Dates related to an individual, including treatment date, admission date, age over 89 or any elements of dates (including year) indicative of such age, date of birth, or date of death [a range of dates (e.g., May 1 – 31, 2021) is permitted provided such range cannot be used to identify the individual who is the subject of the information]
4. Telephone numbers
5. Fax numbers
6. E-mail addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
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
16. Biometric identifiers (e.g., finger and voice prints)
17. Full face photographic images and comparable images
18. Any other unique identifying number, characteristic, or code:
  - that is derived from information about the individual
  - that is capable of being translated so as to identify the individual, or
  - if the mechanism for re-identification (e.g., the key) is also disclosed

In addition, the information provided to CODA cannot be capable of being used alone or in combination with other information to identify the individual.

## FULL DISK ENCRYPTION AND ERASING HARD DRIVES

There are a number of appropriate Full Disk Encryption products available, but here are a few suggestions:

- If you're using Windows 10 Pro or Enterprise, Windows 8 Pro or Enterprise, Windows 7 Ultimate or Enterprise, or Vista Ultimate or Enterprise, you can enable the built in Bitlocker software, which provides Full Disk Encryption.
- If you're a Macintosh user, Apple's OS X version 10.9 (called "Mavericks") and newer (10.10 – "Yosemite", 10.11 "El Capitan", 10.12 "Sierra") includes an enhanced version of a tool called FileVault. This version of FileVault includes a Full Disk Encryption feature that is -FIPS 140-2 compliant. OS X Mavericks shipped in October 2013.
- Another product available for either Windows or Macintosh computers is Symantec's Endpoint Encryption (powered by PGP Technology). This software costs about \$100 per computer and gets excellent reviews.
- If you're interested in a product not mentioned above, the way to be sure that the product is appropriate is to see if it is FIPS 140-2 (Federal Information Processing Standards) validated. (Some FDE software may be appropriate, but might not be FIPS 140-2 validated. If you have questions, please contact the HIPAA Security Official.)

Note:

- When you install Full Disk Encryption, be sure to be extra vigilant about doing regular backups. 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. When you perform those backups, be sure to encrypt them.

There are also a number of ways to securely erase your hard drive, here are a few suggestions:

- 1) If the computer's hard drive had full disk encryption, you can use the Full Disk Encryption utility to erase the drive. You may have to reinstall the operating system to accomplish this.
- 2) Alternately, follow the instructions as appropriate within this article <https://www.tomshardware.com/how-to/secure-erase-ssd-or-hard-drive>
- 3) As a last resort, remove the hard drive and destroy it. This applicable for hard drives with moving parts (platters) or solid state hard drives.
- 4) Whenever possible, apply the recommendations in NIST publication 800-88, available at <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>

Any type of storage device that cannot be erased per NIST publication 800-88 (due to failure, lack of drivers, etc.) should be physically destroyed. Hard drives with moving parts must be disassembled, with platters degaussed and electronics destroyed. Small electronics (SSD hard drives, USB memory, SD RAM chips, Compact Flash) must be destroyed with a hammer using appropriate safety precautions, including safety glasses.