CODA PRIVACY AND DATA SECURITY

TRAINING MANUAL

Effective September 23, 2025

CODA employees and volunteers ("workforce members") must comply with the Policies and Procedures in this Training Manual. This Training Manual includes, but is not limited to, certain CODA HIPAA Policies and Procedures. Federal law requires CODA to train workforce members and to impose sanctions on workforce members who do not comply with CODA's HIPAA Policies and Procedures.

Telephone numbers:

Security Official:	Dr. Kathleen Hinshaw, 312-440-2940
Back Up Security Officials:	Ms. Kelly Stapleton, 312-440-2721
	Mr. Shawn Morrison, 312-440-4681
Building Management Office:	312-329-1275
Building Security Hotline:	312-595-2448

What kinds of information does this Training Manual pertain to?

1. **Sensitive Personally Identifiable Information ("SPI"), such as an individual's name or initials and any of the following**:
   - Social Security number
   - Credit or debit card number or other information (e.g., expiration date, security code)
   - Drivers' license number
   - Financial account number
   - Health insurance information, such as policy number or subscriber I.D.
   - Medical information, such as information about an individual's condition or treatment
   - Mother's maiden name
   - Taxpayer ID number
   - 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. **Protected Health Information ("PHI") and electronic PHI ("ePHI"). This refers to information that identifies an individual (or can be used to identify an individual), that relates to physical or mental health condition, treatment, or payment for healthcare, and that was created or received by a health care provider, health plan, or employer. When in doubt, treat all health information as PHI.**
   a. **PHI includes "genetic information," which is generally defined as:**
      i. **information about a patient's genetic test**

ii. **information about the genetic test of a patient's family member (including a fetus carried by the patient or a family member, or an embryo legally held by a patient or family member utilizing an assisted reproductive technology)**

iii. **the manifestation of a disease or disorder in a patient's family member**

iv. **any request for, or receipt of, genetic services by a patient or a patient's family member ("genetic services" means a genetic test, genetic counseling, or genetic education), or**

v. **any request for, or receipt of, participation in clinical research that includes genetic services by a patient or a patient's family member.**

b. **Identifiers.** Information identifies, or can be used to identify, a patient if the information either:

i. can be used, alone or in combination with other information, to identify an individual, or

ii. contains one or more of 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 smaller than a state (including street address, city, zip code, county, precinct)

3. Dates directly related to the individual, such as treatment date, admission date, age, date of birth, or date of death [a range of dates (e.g., May 1 – 31, 2015) is permitted provided such range cannot be used to identify the individual who is the subject of the information], and ages over 89.

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

Institutions have been instructed to provide PHI/SPI to CODA workforce members at site visits ONLY, and not to transmit PHI/SPI via U.S. mail, email, USB Drive, etc. If you receive PHI/SPI outside of a site visit, notify the Security Official IMMEDIATELY (hinshawk@ada.org, stapletonk@ada.org, or morrisonsh@ada.org) and protect the information from use or disclosure until you have completed the Security Official's instructions concerning the PHI/SPI.

CODA workforce members must de-identify all PHI and remove all SPI in any report or other documentation that they prepare for CODA.

1. About CODA's Privacy and Data Security Policies and Procedures

a. All CODA workforce members must be aware of, understand, and follow the CODA HIPAA Compliance Policies and Procedures and the information in this Training Manual.

b. Privacy and Data Security law violations can result in stiff penalties and, in some cases, criminal prosecution.

c. CODA will provide a copy of the CODA HIPAA Compliance Policies and Procedures and this Training Manual to each workforce member. The Policies and Procedures and Training Manual will be posted on the Commission's internal document retention platform (Knowledge Center/SharePoint) and may be requested from the CODA Security Official.

2. **Documentation**

   a. The Security Official will provide any documentation necessary for CODA employees and volunteers ("workforce members") to implement the CODA HIPAA Compliance policies and procedures and the requirements of this Training Manual.

   b. Workforce members must give any HIPAA and/or Privacy and Data Security documentation that they acquire or create to the Security Official for retention.

3. **In the CODA Facility**

   a. Do not allow unauthorized individuals into the CODA facility.

   b. Visitors must be supervised at all times.

   c. Comply with facility security rules (key card access, etc.). Report problems with doors and locks to Building Management, and security problems (such as suspicious individuals) to the Building Security Hotline.

   d. Do not leave key cards unattended, or leave electronic devices (including phones) unattended without logging off.

   e. Computers containing electronic protected health information ("ePHI") may not be used away from controlled areas where only workforce member users and other authorized users have access.

   f. Electronic fax machines must only be accessed by authorized CODA staff using strong passwords. Electronic faxes that contain ePHI must be securely deleted.

   g. Do not move your desktop computer without the Security Official's approval.

   h. Do not allow unattended visitors to enter nonpublic areas of the facility where there is access to PHI or SPI. Supervise visitors at all times.

   i. Your computer and all PHI/SPI should not be visible to persons who are not authorized to access the information.

   j. Hard copy PHI/SPI (paper, films, microfiche, etc.) must be stored in designated locked file cabinets or records rooms and must not be removed from the CODA facility without the Security Official's approval. When appropriate to dispose of hard copy PHI/SPI, these materials must be disposed of securely (e.g. in a locked recycling bin).

4. **Outside the CODA Facility**

   a. Avoid unnecessary disclosures of PHI/SPI by keeping voices low when discussing PHI/SPI in public.

   b. Be alert for unauthorized listeners.

   c. Avoid using patients' names in public areas.

   d. Conduct dictation and telephone conversations away from public areas.

   e. Only use speaker-phones in private areas.

   f. Do not leave a computer that has been used to access PHI/SPI unattended without logging off.

   g. Never leave a laptop unattended unless it has been secured with a cable lock according to the manufacturer's instructions.

   h. 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.

   i. A CODA employee may not remove PHI/SPI on paper or on removable media from the CODA facility unless he or she is authorized to do so by the Security Official and has received Privacy and Data Security training. Use reasonable and appropriate means to protect the privacy and security of the PHI/SPI on paper or removable media, including keeping them under your control or locked in a secure container when not in use, only saving PHI to removable media if it is (1) authorized by CODA and (2) saved in an IT-approved encrypted format (see Appendix C), and following the safeguards listed for laptops in section 6.

   j. On occasion, an educational program may request historical records from the

Commission office (also known as legacy documents). Legacy documents may only be provided to programs when (1) authorized to do so by the Security Official, and (2) saved and transmitted in an IT-approved encrypted format (see Appendix C).

5. Passwords

Whenever CODA requires you to use a password, the following rules apply:

a. Workforce members must understand and adhere to all CODA password requirements.

b. Never share a password.

c. Choose a "strong password": passwords must be at least eight (8) characters in length, a mix of upper and lower case letters, numbers and symbols, and should be a word that cannot be found in the dictionary (Staff password protocol found at DES_PasswordRequirements.docx).

d. If you write down a password, store it securely under lock and key. Do not keep it with the laptop or other device, or post it anywhere.

e. Change your passwords at least four times a year.

f. Change your password whenever you are prompted to do so, and whenever CODA or the ADA Department of Information Technology ("IT") asks you to do so.

g. Set your Internet browser so it does not "remember" passwords.

h. If IT asks you to give a password to someone who is providing technical support, you must change the password immediately after such support is finished.

i. If IT must assign a temporary password to someone who is not an ADA employee (for example, a contractor or vendor working on the deployment of new hardware) the password must be de-activated immediately when deployment is complete.

j. Your password to access information on ADA systems and devices will be deactivated when your assignment is over or when you change jobs and no longer require access to CODA information.

k. Change any initial assigned passwords to user-selected passwords on initial login (for example, you must change your password from the default value assigned by a network administrator).

l. Protect any computer that you use to access CODA information with a login password (including your own laptop or desktop computer).

6. **Laptop Security.**

If you use a laptop for your CODA work you must follow these procedures (whether or not the laptop is the property of the ADA):

a. 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) 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.

b. Never leave your laptop unattended without logging off and securing the laptop with a cable lock according to the manufacturer's instructions.

c. Store your laptop locked and out of sight (for example, lock it in the trunk of a car rather than on the back seat). However, if you lock your laptop in a car trunk, move the car to a new location that is out of sight of the original location, in order to help prevent a break-in by an observer.

d. CODA requires full disk encryption of laptops (see Appendix A for information and instructions). Use a strong password (see above).

e. Set your laptop to automatically lock or log off after fifteen (15) minutes of inactivity.

f. If your computer is lost or stolen contact the police and call the Security Official **immediately** at 312-440-4653 (the CODA main office number).

g. Do not connect a computer not owned by the ADA to the ADA local area network.

7. **Computer and Internet use**

   a. Never access ePHI using anything other than a secured desktop or laptop computer. For information on securing a desktop or laptop, see Appendix A.

   b. CODA materials that do not contain ePHI may also be viewed on ADA Connect using your smartphone, tablet, or similar device. You must use a strong password to secure the device. For information on securing an iPad, see Appendix D. If you have an Android tablet, contact CODA for further instructions.

   c. Never download or print PHI/SPI unless you are an ADA employee using an ADA computer.

   d. ADA employees using ADA computers must avoid downloading PHI/SPI. If an ADA employee must download PHI, the data file should be encrypted (see section 7).

   e. 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.

   f. Do not have any other Internet browser windows open while accessing ePHI/SPI on a computer.

   g. Never access ePHI/SPI if passersby or other unauthorized individuals are able to view the ePHI/SPI.

   h. If you are a CODA volunteer who accesses ADA Connect or ePHI/SPI from your own computer (desktop or laptop) or if you are a CODA staff who accesses ADA Connect, Knowledge Center or ePHI/SPI from your own computer you must:

      1) protect your computer with antivirus software that has up-to-date signature files

      2) protect your computer with anti-malware and anti-spyware software

      3) Protect your computer with full disk encryption ("FDE"). See Appendix A for more information on FDE.

4) have all recent relevant security fixes applied, including fixes for operating system, Internet browser, and major applications such as Acrobat Reader and Microsoft Office

5) before permitting a repair technician, tech support, or other individual to service or repair the computer, have an appropriate signed Business Associate Agreement in place with the applicable entity or person

i. Do not install or download onto an ADA computer any unauthorized software or data. Volunteers and staff must not use peer-to-peer file sharing software, such as Kazaa, Morpheus, Dropbox, LimeWire, or BitTorrent, on any computer that they use for CODA work.

j. Backups of computers that access ePHI/SPI or store unencrypted ePHI/SPI must be encrypted using a strong password and AES 128 bit encryption at a minimum.

k. Other than direct access to PHI/SPI on-site during a site visit, access to electronic PHI/SPI must not be provided. If an institution provides documents (electronic or paper) containing PHI/SPI directly to you, notify the Security Official (hinshawk@ada.org, stapletonk@ada.org, and morrisonsh@ada.org) immediately.

l. Do not e-mail PHI/SPI to anyone. Exception: ADA employees may e-mail unencrypted PHI/SPI to other ADA staff using internal ADA e-mail addresses only.

8. Electronic Media

a. Do not save PHI/SPI to removable media (i.e., CDs, DVDs, external USB hard drives, USB memory sticks, USB thumb drives, SD-RAM chips, Compact Flash memory chips, etc.) because they are easy to lose.

b. CODA prohibits institutions from sending PHI/SPI to CODA workforce members. If an institution sends you anything containing PHI/SPI, notify the

Security Official (hinshawk@ada.org, stapletonk@ada.org, and morrisonsh@ada.org) immediately.

c. Any volunteer who has removable media containing unencrypted PHI/SPI must safeguard the PHI/SPI as follows:

1) If the PHI/SPI is no longer needed and it is stored on re-writeable media:

a) delete it from the place where it is stored using “Shift-Delete” (so it doesn’t end up in the recycle bin)

b) if possible, perform a secure wipe of the media (see Section 9)

2) If the PHI/SPI is no longer needed and it is stored on write-once media (e.g., CD-ROM, DVD-ROM), appropriately dispose of the write-once media (see Section 9)

3) If the PHI/SPI is still needed, encrypt it (see Appendix C)

d. CODA volunteers shall securely dispose of data after they have reviewed and approved the preliminary draft site visit report. CODA volunteers must not retain any program or CODA materials beyond their intended use to conduct work on behalf of CODA. In all other cases, the Security Official will determine when protected health information may be destroyed. Any CODA workforce member who is authorized by the Security Official to dispose of electronic or hard copy PHI/SPI shall follow these instructions:

1) <u>Shred paper documents</u> so that they cannot be read or reconstructed. If you use a document destruction firm to shred your documents:
   a) <u>Store documents in a securely locked bin prior to shredding</u>
   b) <u>Confirm that a compliant business associate agreement is in place with the document destruction firm</u>
   c) <u>Confirm that the firm destroys documents so that the documents cannot be read or otherwise reconstructed</u>
   d) <u>Verify identity of the recycling firm representative as appropriate</u>
2) <u>Shred CDs</u>
3) <u>For data stored on external USB drives:</u>
   a) If the files containing Sensitive Information or Patient Identifiers are encrypted, or if the external USB drive is itself encrypted

        i. Simply delete those files, following the instructions below titled "Securely Delete files from your computer"
    b) 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:
        i. 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.
        ii. 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)
            a. For USB drives that have moving parts, i.e. external hard drives, contact CODA for additional instructions

4) <u>"Securely Delete" files from your computer</u>:
    a) To securely delete a file if you are using Windows:
        i. Click once on the file to highlight it but not open it
        ii. Click "shift" and "delete" to permanently delete the file
        iii. Check your Recycle Bin to ensure the file is permanently deleted. If it appears in the Recycle Bin, delete it again
    b) To securely delete a file if you are using a Mac:
        i. Delete the file
        ii. Go to your Mac's Finder menu (upper left-hand side of your screen)
        iii. Choose "Secure Empty Trash..."
5) <u>"Securely Delete" an email:</u>
    a) Click once on the email to highlight it but not open it
    b) Click "shift" and "delete" to permanently delete the email
    c) Check your Deleted Items Folder to ensure the email is permanently deleted. If it appears in the Deleted Items Folder, delete it again
6) <u>"Securely Delete" an attachment from your email:</u>
    a) Open the email
    b) Click on the attachment to highlight it but not open it
    c) Click "shift" and "delete" to permanently delete the attachment
    d) Check your Deleted Items Folder to ensure the file is permanently deleted. If it appears in the Deleted Items Folder, delete it again

9. De-Acquisition

Before you get rid of (throw away, give away, sell, reassign, etc.) a laptop or desktop computer that has been used to access PHI/SPI:

a. If the computer is owned by the ADA, IT will wipe it before it is reassigned or de-acquired.

b. If the computer is not owned by the ADA, and if the computer was used to access PHI/SPI, you must thoroughly erase the hard drive of your computer following the procedures specified by IT before the computer is de-acquired:

   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, you can remove the hard drive and destroy it. This applicable for hard drives with 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

c. 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 (see Section 13 "Destruction of PHI/SPI") using appropriate safety precautions, including safety glasses.

d. If ePHI/SPI has been saved to removable media, follow instructions in section 8.d above.

10. Examples of things that you must report immediately to the Security Official: Contact the CODA security officials (hinshawk@ada.org, stapletonk@ada.org, and morrisonsh@ada.org) immediately if you discover:

a. 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.

b. Any “security incident,” sign of intrusion, or suspected compromise to Knowledge Center or ADA Connect. A *security incident* is “the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.” Report any suspected or known security incident to the Security Official as soon as discovered. Contact the Security Official and IT if you suspect a compromise to the system.

c. Any possible or suspected “breach” of PHI/SPI. A breach is generally defined as the unauthorized acquisition, access, use, or disclosure of unsecured PHI/SPI. Examples of possible breaches include:

1) throwing a CD containing unencrypted PHI/SPI away in a wastebasket

2) losing a laptop that has been used to access PHI/SPI

3) showing ePHI/SPI to a colleague who is not authorized to access it

4) discussing PHI/SPI with a friend who is not authorized to access it

5) accidently leaving a memory stick with unencrypted ePHI/SPI on a store counter

6) leaving a paper document containing PHI/SPI in the public area of an office

d. Any use or disclosure of PHI/SPI for any purpose other than accreditation of the institution.

e. Any individual’s request (such as a patient or patient’s representative) to:

1) access PHI

2) amend PHI, or

3) for an accounting of disclosures of PHI

(Do not grant the request—tell the individual you must refer the request to the Security Official)

f. Any request or communication from the U.S. Department of Health and Human Services, the Office for Civil Rights, or a state attorney general.

g. Any problem with security at the ADA facility (locks, electronic passes) that could affect the security of ePHI/SPI.

h. Any PHI/SPI that is unavailable or that appears to be altered, damaged, or corrupted.

i. Any complaint about security, privacy, or CODA's privacy and security policies and procedures.

j. Any suspected violation of CODA's HIPAA Compliance Policies and Procedures or the requirements of this Training Manual.

k. Any pattern of activity or practice of an institution or a vendor or subcontractor that appears to constitute a material breach or violation of the institution's obligations concerning privacy or security.

l. Any institution's breach or violation of its obligations to CODA.

m. Any suspected unauthorized use of or access to PHI/SPI.

n. Any misdirected e-mail, U.S. mail, or courier delivery containing PHI/SPI.

o. Any PHI/SPI that you receive other than PHI/SPI accessed onsite during a site visit.

11. De-identifying PHI

a. Do not include any patient information (even de-identified PHI) in a site visit report or any other CODA document.

b. Do not use redaction (e.g., black marker) to de-identify PHI.

c. Patient information is not "PHI" if it has been properly de-identified. How to de-identify PHI:

Step 1: Remove all 18 identifiers of the individual (e.g., the patient) and his or her relatives, employers, or household members:

1. Names, including initials

2. Address information smaller than a state (including street address, city, zip code, county, or precinct)

3. All elements of dates directly related to an indivdiual, such as treatment date, admission date, age, date of birth, or date of death [a range of dates (e.g., May 1-31, 2015) is permitted provided such range cannot be used to identify the individual who is the subject of the information], and ages over 89

4. Telephone numbers

5. Fax numbers

6. Electronic 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, 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 number, characteristic, or code:

a. that was derived from information about the individual,

b. that is capable of being translated so as to identify the individual, or

c. if the mechanism for re-identification (e.g., the key) is also disclosed.

Step 2: Make sure you do 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.

12. Access to PHI/SPI

a. You are only authorized to access the PHI/SPI that is necessary for your job or assignment.

b. Your username and password should only allow you access to the PHI/SPI you need for your job or assignment.

c. When your job or assignment ends, your access will be de-activated.

d. Never share your username or password.

e. CODA volunteers may only access PHI/SPI on site.

f. Never grant access to Knowledge Center/SharePoint or ADA Connect to an unauthorized individual.

g. CODA volunteers may not download or make hard copies of PHI/SPI.

h. If you are authorized to use, request, or disclose PHI/SPI, disclose the minimum amount necessary for the purpose of the use, request, or disclosure.

i. Immediately notify the Security Official if you become aware of any disclosure of PHI for purposes other than accreditation. The Security Official may be required to log the disclosure to be prepared to provide an accounting of disclosures of an individual’s PHI (see Appendix B).

j. An ADA employee or volunteer must get the Security Official’s approval before either:

1) disclosing PHI/SPI to an unauthorized individual (or allowing an unauthorized individual to use or access PHI/SPI) or

2) allowing a contractor, vendor's representative, tech support person, etc. to access PHI/SPI, a system with PHI/SPI, or a device that has been used to access PHI/SPI

However, an ADA employee in IT may allow a contractor, vendor's representative, tech support person, etc. to access PHI/SPI, a system with PHI/SPI, or a device that has been used to access PHI/SPI provided the employee confirms (1) that an up-to-date Business Associate Agreement is in place, and (2) the contractor, vendor's representative, tech support person, etc. has been counseled on CODA HIPAA Compliance Policies and Procedures.

k. If you are authorized to disclose or allow access to someone you don't know, confirm or validate the individual's identity and authority (for example, check a tech support contractor's ID).

13. Etcetera.

a. Never make any changes to PHI/SPI.

b. Never fax PHI/SPI.

c. If you are assigned responsibilities under a disaster plan, emergency plan, or contingency plan, learn your responsibilities and carry them out as appropriate.

d. Do not use or disclose PHI/SPI for connection with marketing communications, or give PHI/SPI to anyone else to send a marketing communication.

e. Do not use or disclose PHI/SPI to send fundraising communications.

f. Do not disclose PHI/SPI to anyone who is not authorized to receive it, and even if another individual is authorized to receive PHI/SPI, do not disclose PHI/SPI in exchange for any kind of remuneration without the prior approval of the Security Official.

APPENDIX A

Full disk encryption

What is "Full Disk Encryption" (or FDE)?

- It is a security tool that unobtrusively encrypts your entire computer hard drive
- This encryption secures your hard drive so that no one can access it without a valid password.
- This tool becomes important to you if your computer is lost or stolen.

The password you already use to log onto your computer isn't enough. Why not?

- Unfortunately, neither your Windows nor your Macintosh password does a good job of protecting your data.
- Even though your computer is protected by a password, it is still relatively easy for someone to access your data. They don't need to know your password to do so. They only need physical access to your computer and a little bit of technical knowledge.
- One way is to boot another operating system from your CD-ROM drive or from a USB drive.
  For example, a person who has your computer can boot a copy of Linux from a USB drive and then access your Windows or Macintosh hard drive the same way you would access any USB drive.
- Another way is to remove your hard drive from your computer and temporarily attach it to another computer, again sort of like a USB drive.
- In either case, any file on your computer could be accessed without your permission or knowledge, if someone had possession of your computer.

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".

How Full Disk Encryption works

- You first obtain Full Disk Encryption software and install it.
- The software uses a password that you provide to encrypt your entire computer's hard drive.
- When you start up your computer, you may be prompted for a boot up password (this is an option for some software). If not, you will be prompted for your usual login password (which should also be a strong password.)
- If a person tries to boot another operating system and access your files, they will not be able to see any data because they do not have the encryption password.
- If a person removes your hard drive and tries to access the files, they will not be able to see any data because they do not have the encryption password.
- In order to access a hard drive that has been encrypted using Full Disk Encryption, you need to know either the encryption password or a valid login password, depending on the configuration.

Where can I obtain Full Disk Encryption software?

There are any number of appropriate 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, the newest version of Apple's MacOS (10.12) called "Sierra" includes an enhanced version of a tool called FileVault. FileVault includes Full Disk Encryption functionality. MacOS Sierra shipped in September 20, 2016. File Vault is also included in earlier versions of Apple's OS X ("El Capitan" 10.11, "Yosemite" 10.10, "Mavericks" 10.9).
- Another product available for either Windows or Macintosh computers is Symantec's Drive Encryption (powered by PGP Technology). This software costs about $100 per computer.

If you wish to use FDE software that is not listed here, please make sure that the FDE software complies with one of these standards:

- It is FIPS 140-2 (Federal Information Processing Standards) validated. We are unaware of any FDE software that is not FIPS 140-2 validated, but you should verify.
- Alternately, confirm that your FDE software uses AES encryption with 128 bit keys or longer.

After you've installed Full Disk Encryption:

- Don't forget your password. If you do, you may lose data.
- Do regular backups of the computer protected with FDE. If you have a hard drive failure, it will be fruitless to send your hard drive to a vendor to try to recover data files.
- When you perform those backups, be sure to encrypt them using a strong password and AES 128 bit encryption at a minimum.

APPENDIX B

LOG OF DISCLOSURES OF PHI

If a CODA employee or volunteer discovers that PHI has been used or disclosed for a purpose other than accreditation, he or she must immediately notify the Security Official. If any such notifications are received, the Security Official must complete the following log.

Name of CODA employee or volunteer:____

Date of disclosure	Who received the PHI: name and address (if known)	General description of the type of PHI disclosed[1]	Purpose of the disclosure

[1] Give a general description of the type of PHI that was disclosed (such as “name” or “social security number”). Do not write the actual PHI on this form.

APPENDIX C

Encrypting Commonly Used Files

To password protect an Excel spreadsheet, using Excel 2010 or newer:

1. Open the Excel spreadsheet
2. Click on the "File" tab (located in upper left hand corner of the application)
3. Click on "Info", then "Protect Workbook"
4. Select "Encrypt with Password"
5. Enter a strong password*
6. Re-enter the strong password
7. Save the file in the default Excel format (.XLSX), not as an Excel 97-2003 file (.XLS)

To password protect a Word document, using Word 2010 or newer:

1. Open the Word document
2. Click on the "File" tab (located in upper left hand corner of the application)
3. Click on "Info", then "Protect Document"
4. Select "Encrypt with Password"
5. Enter a strong password*
6. Re-enter the strong password
7. Save the file in the default Word format (.DOCX), not as a Word 97-2003 file (.DOC)

To password protect an Adobe Acrobat (PDF) document, using Acrobat X (or newer) Standard:

(Please note: you can only encrypt Acrobat documents if you have Acrobat Standard or Acrobat Professional. The free Acrobat Reader software does not include document encryption.)

1. Open the Acrobat document
2. Select "File", then "Properties"
3. Select the "Security" tab
4. For the "Security Method", select "Password Security"
5. For "Compatibility", select "Acrobat 7.0 and later"
6. Make sure the "Encrypt all document contents" button is selected
7. Check the "Require a password to open the document" checkbox
8. Enter a strong password*
9. Re-enter the strong password
10. Save the file

To password protect a file or group of files that are not encrypted using one of the methods outlined above, you must use WinZip version 16 or newer. You must use the AES-2 encryption method with 256 bit keys or 128 bit keys. Earlier versions of WinZip are insecure, and earlier versions of WinZip encryption (such as Zip 2.0 encryption) are insecure. Please request ADA document "Winzip encryption" for further details.

When you transmit an encrypted document via email, provide the password separately, preferably by phone. Do not provide the password in the transmittal email with the document! If you provide the password via separate email, securely delete the email containing the password after you send it (see below).

To securely delete an email containing PHI or SPI or a password:

1. Delete the email message
2. Go to “Deleted Items” (or similar), find the email, and delete it
3. If you use Outlook, go to “Tools” and click on “Recover Deleted Items.” If the email is there, delete it.

If someone sends you PHI/SPI via email, securely delete the email after you have made a hard copy or entered the PHI/SPI in the document. Store hard copy PHI/SPI under lock and key.

Please note: The password protection in versions of Excel and Word earlier than their Office 2007 versions is not secure enough to protect PHI/SPI. Also, the password protection in versions of Acrobat Reader earlier than version 7 is not secure enough to protect PHI/SPI. Finally, if you forget the password for a password encrypted Excel, Word, or Acrobat file, there is no way to reset the password or any other way to open that file.

*Suggestions for constructing a strong password:

- Your password should be at least eight characters long. Ten or twelve is better.
- Your password should be complex – by this we mean you should use all of these types of characters: lower case letters, upper case letters, punctuation symbols, and numbers.
- Your password must not be:
    - A single word
    - A word that can be found in an English or foreign language dictionary
    - The name of a famous person or fictional character
    - Words that are part of user names (for example, your name or the name of your council)
    - Doubling up of certain small words (for example, “golfgolf”)
    - Patterns that are commonly used as passwords (“12345678”, “qwerty”, “asdfgh”, etc.)
    - Prefixing or suffixing any word found in sources listed above with numbers (for example “1password” or “password1”)

APPENDIX D

Using an iPAD to access PHI/SPI

If you wish to use an iPad to access PHI/SPI, you must perform all of the following steps to electronically secure your iPad:

1. Configure your iPad so that a password is required for access. You must use a “strong password”, not just a 4 digit passcode. See further instructions in Appendix C of this document.
2. By default, the maximum number of failed login attempts is 10. Do not change this setting.
3. By default, your iPad is configured to erase all data if the maximum number of failed login attempts occurs. By default, this will occur after 10 attempts. Do not change this setting.
4. Make sure the iPad is registered with either iCloud or a Microsoft Exchange Server. Either service will allow you to perform a “Remote Wipe” if your iPad is lost.
5. If you backup your iPad to a computer using iTunes, you must encrypt your backup. It is not encrypted by default. (In the iTunes Summary screen, select "Encrypt iPhone backup".) Alternately, you may use FDE (Full Disk Encryption) on the computer that you use to back up your iPad. However, if you have FDE enabled and do not encrypt your iTunes backup to your hard drive, you must then encrypt any external backups (to tape, to another hard drive, to a cloud backup service) of your computer hard drive.

How to perform a “Remote Wipe” if your iPad is connected to your organization’s email server

If you have an iPad (or iPhone, Android phone, Android tablet, Windows Mobile phone) that syncs your organizations email on it, you may be able to use OWA (Outlook Web Access) to wipe all data from your device if your device is lost or stolen. Here is how to do that:

1. Sign in to your organization’s web mail service. It is often titled “OWA”, and may have a URL similar to this: http://owa.mycompany.com.
2. Click on “Options” in the upper right corner of the web mail window
3. Click on “Mobile Devices” from the list of options on the left side of the screen
4. Click to highlight the device that was lost. If you have more than one device listed, you can determine which is the one that was lost by looking at the “last sync time”, or by clicking on the “+” sign to expand the details. You should be able to see a description of your device in the details.
5. Once you’ve identified the lost device, make sure it’s highlighted, then click on “Wipe All Data from Device”. When prompted if you are sure, click on “OK”
6. If your device is connected to a cellular or wi-fi network, it will receive the erase command and will be erased.

Please take a few minutes now to log in to your organization’s web mail service and walk through the steps 1 – 4 above. This will help you to remember the process if your device is lost. Please contact your organization’s IT department if you have any questions about this procedure.

How to perform a “Remote Wipe” if your iPad is connected to Apple’s iCloud

1. Follow these instructions from Apple: http://support.apple.com/kb/PH2701?viewlocale=en_US

Please take a few minutes now to review the instructions at the link above so that you can confirm that your iPad is configured correctly, and that you are familiar with the necessary steps. This will increase the possibility that this process will be successful when it is needed.

Regarding Encryption and the iPad

- All data stored on the iPad is encrypted at rest. The iPad uses 256-bit AES encoding hardware-based encryption to protect all data on the device. Encryption is always enabled and cannot be disabled by users.

If your iPad contains PHI/SPI and is lost

CODA does not permit volunteers to download PHI/SPI to an iPad (or other device). However, if you have followed the instructions above to secure your iPad, and your iPad is lost, then any PHI/SPI contained in the iPad would be considered “secure”.

However, you must still report this loss to security officials as a potential breach, as explained in section 10 of the Training Manual.