

COMMISSION ON DENTAL ACCREDITATION
HIPAA COMPLIANCE POLICIES AND PROCEDURES
EFFECTIVE DATE: September 23, 2025

1. The CODA Security Official

- a. **Security Official.** The Director of the Commission on Dental Accreditation will be the CODA Security Official. The Security Official shall develop and implement the policies and procedures for CODA's compliance with the HIPAA Security, Privacy, and Breach Notification Rules, and shall be responsible for receiving any inquiries, requests, and complaints regarding CODA's HIPAA compliance.
- b. **Backup Security Official.** The CODA Predoctoral Dental Education, and Training and Assessment managers will be the backup Security Official who shall take responsibility for that role in the event the Security Official is ill, on vacation, or otherwise unable to respond to a security situation.
- c. **Delegating tasks.** The Security Official may delegate tasks and responsibilities but shall retain ultimate responsibility and accountability for CODA's compliance with the HIPAA Security Rule.

2. Business Associate Agreement

CODA shall enter into an appropriate Business Associate Agreement with each institution that CODA accredits; the Business Associate Agreement shall specify that the agreement is effective only if (and then only to the extent that) the Commission is the Institution's Business Associate or Subcontractor under HIPAA. Any downstream Business Associates shall be required to enter into Business Associate Agreements when contracting with the ADA.

3. Policies and Procedures

The Security Official shall implement reasonable and appropriate policies and procedures to comply with applicable HIPAA Standards and Implementation Specifications, taking into account:

- a.** CODA's size, complexity, and capabilities
- b.** CODA's technical infrastructure, hardware, and software security capabilities
- c.** The costs of security measures
- d.** How likely and how critical a potential risk to CODA's electronic protected health information as defined by HIPAA ("ePHI") would be

The Security Official may change the policies and procedures at any time, provided that the changes are documented and are implemented in compliance with HIPAA. The policies and procedures shall be set forth in these CODA HIPAA Compliance Policies and Procedures and in the CODA Privacy and Data Security Compliance Training Manual (the "Training Manual").

4. Documentation

The Security Official shall document and maintain, in hard copy and/or electronic form, CODA's HIPAA policies and procedures, a record of any action, activity, or assessment that HIPAA requires to be documented.

- a. Time Limit.** The Security Official shall retain the documentation for at least six years from the date of its creation or from the date when it was last in effect, whichever is later.
- b. Availability.** The Security Official shall make the applicable documentation available to those persons responsible for implementing the procedures and as required by law.

- c. Updates.** The Security Official shall review the documentation periodically, and update as needed in response to environmental or operational changes affecting the security of the ePHI.

5. Risk Analysis

- a. Initial Risk Assessment.** The Security Official shall conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the ePHI that CODA holds.
- b. Periodic Updates.** The Security Official shall periodically update the risk analysis whenever he or she determines that risks or changes in CODA's operating environment or in the regulatory environment warrant review.

6. Risk Management

The Security Official shall implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to:

- a.** Ensure the confidentiality, integrity, and availability of all ePHI that CODA creates, receives, maintains, or transmits
- b.** Protect against any reasonably anticipated threats or hazards to the security or integrity of such ePHI
- c.** Protect against any reasonably anticipated uses or disclosures of such ePHI that are not permitted or required under the HIPAA Privacy Rule
- d.** Ensure compliance with the Security Rule by the CODA workforce

7. Workforce Training, Sanctions, and Complaints

- a. Training and Sanctions.** The Security Official shall set forth policies and procedures that apply to CODA workforce members in the Training Manual, which shall be distributed to each workforce member. The Security Official shall train workforce members to comply with CODA's HIPAA policies and procedures, and the

Training Manual shall state that sanctions will be imposed if a workforce member violates CODA's HIPAA policies and procedures. The Security Official shall investigate any suspected incident of which he or she becomes aware and shall apply appropriate sanctions against workforce members who fail to comply with CODA HIPAA policies and procedures. No sanctions may be imposed against workforce members whose reason for the conduct is in good faith and in accordance with HIPAA Privacy Rule provisions, such as a whistleblower reporting to a government agency, or a workforce member crime victim reporting to a law enforcement official.

b. Institutions' Evaluations. Following a site visit, institutions will be asked to evaluate site visitors and site visitors will be asked to evaluate each other. A negative evaluation with regard to these policies and procedures may result in sanctions.

c. Forms of Sanctions. If a workforce member appears to have violated a CODA HIPAA policy or procedure, the Security Official shall investigate. If the Security Official concludes that a violation has occurred, the Security Official shall apply an appropriate sanction. Examples of possible appropriate sanctions include:

- (1) having a private conversation with the workforce member to review the appropriate safeguards and make sure that the workforce member understands the policy
- (2) written reminder
- (3) additional mandatory training

- (4) telling the workforce member that any further violation will involve suspension, and place a letter of warning of suspension in the workforce member's file
- (5) Suspension without pay and placement of a letter of warning of termination in the workforce member's personnel file
- (6) Termination

d. Complaints. CODA's complaint process is documented in the online EOPP Manual.

8. Reviewing Activity on Information Systems

Whenever IT provides the Security Official with a security incident tracking report that indicates possible inappropriate activity in connection with CODA ePHI, the Security Official shall regularly review such reports and, in consultation with IT and Legal, determine an appropriate course of action.

9. Workforce Security

The Security Official shall implement policies and procedures to ensure that all members of the CODA workforce have appropriate access to ePHI and to prevent those workforce members who should not have access to ePHI from obtaining access.

- a. Authorization.** The Security Official shall implement procedures for the authorization of workforce members who work with ePHI or in locations where ePHI might be accessed. Employees of the American Dental Association (ADA) who are authorized to access PHI have written job descriptions that define appropriate access. CODA volunteers are assigned access to ePHI based on their assignments. CODA requires institutions to provide access to PHI and ePHI on site only, and prohibits institutions from transmitting PHI or ePHI to

CODA. Password protections on FileWeb, Knowledge Center, and ADA Connect prevent unauthorized individuals from accessing ePHI.

- b. Clearance.** The Security Official shall determine that the access of each workforce member to ePHI is appropriate and each workforce member will be issued a username and shall choose a password that will allow access only to the ePHI necessary for the job or assignment. The ADA Human Resources Division (HR) is responsible for conducting reference and background checks on workforce members who are ADA employees. The clearance of CODA volunteers is conducted through their nomination by participating communities of interest and appointment by the Commission based on factors including their qualifications.
- c. Termination.** At the end of the employment or assignment of a workforce member who is an ADA employee, the Security Official shall notify the ADA Division of Human Resources (“HR”) and the ADA Department of Information Technology (“IT”) to terminate access to ePHI. When the assignment of a volunteer ends, the ADA Connect CODA Site Administrator terminates access by deleting the applicable user account.

10. Managing Access to Information

The Security Official shall implement policies and procedures for authorizing access to ePHI that are consistent with applicable requirements of the HIPAA Privacy Rule.

- a. Healthcare Clearinghouse.** CODA is not, and shall not use, a clearinghouse as that term is defined under HIPAA.
- b. Authorizing, Establishing, and Modifying Access.** The Security Official shall implement policies and procedures for granting access according to job function to ePHI to workforce members and to representatives of ADA vendors who are

downstream Business Associates. Based on the policies and procedures for granting access, the Security Official shall implement policies and procedures to establish, document, review, and modify a user's right of access to ePHI through a workstation or program.

11. Security Awareness and Training


CODA shall implement a security awareness and training program for all workforce members (including management) that will cover HIPAA Security, Privacy, and Breach Notification policies and procedures, as necessary and appropriate for the workforce members to carry out their functions. Such training shall include distribution of the Training Manual. Training shall be provided to workforce members as necessary.

a. Security Reminders The Security Official may provide periodic security updates reminders to workforce members. For example, the Security Official may:

- (1)** Post reminders on electronic media that contain ePHI
- (2)** Post reminders near electronic media that contain ePHI to which representatives of Business Associates have access
- (3)** Include reminders in written materials distributed to workforce members
- (4)** Announce reminders orally when addressing workforce members
- (5)** Post reminders from time to time on site-use agreements that users are required to agree to in order to sign in

b. Protection from Malicious Software. The Security Official assigns to IT the responsibility to implement procedures for guarding against, detecting, and reporting malicious software on ADA computers. The Security Official shall train workforce members as to the protection required by CODA for computers and devices that are not owned by ADA.

c. Automatic Lock-out, Login Passwords, Laptop Security, and Computer and

- Internet Use.** The Security Official delegates to IT the responsibility to implement technology on ADA computers to impose an automatic lock-out after a certain number of unsuccessful log-in attempts. The Security Official shall train workforce members to protect any computer used to access ePHI with a login password and shall train workforce members regarding automatic lock-out, login passwords, password management, laptop security, computer and Internet use.
- d. Password Management.** The Security Official delegates to IT the responsibility to implement policies and procedures for creating, changing, and safeguarding passwords on ADA computers and for developing password management requirements for CODA workforce members. The Security Official shall train workforce members to comply with password management requirements in  [DES PasswordRequirements.docx](#) and will update training as necessary. The Security Official shall train workforce members to follow password management procedures on ADA Connect.

12. Security Incident Response and Reporting

A *security incident* is defined as “the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.”¹ The Security Official shall train workforce members to promptly report to the Security Official any signs of intrusion and any suspected compromise to the system. Upon receiving such a report, the Security Official shall, in cooperation with IT and the Legal Division, take action to:

- a.** identify and respond to suspected or known security incidents

¹ 45 CFR 164.304.

- b. mitigate, to the extent practicable, harmful effects of security incidents that are known to CODA, and
- c. document the security incident, actions taken to minimize harmful effects, and outcome.

13. Contingency Plan

The Security Official shall establish (and implement as needed) policies and procedures for responding to emergencies or other occurrences (for example, fire, vandalism, system failure, and natural disaster) that may damage systems that contain electronic PHI.

- a. **Data Backup Plan.** The Security Official delegates to IT the responsibility to establish and implement procedures to create and maintain retrievable exact copies of electronic PHI. IT shall back up ePHI nightly and follow a tape rotation schedule that provides access to several weeks of daily backup tapes. IT shall periodically store certain backups at an offsite backup storage facility. If backed up ePHI must be restored the Security Official shall either contact IT or shall request the institution resend the ePHI.
- b. **Disaster Recovery Plan.** The Security Official delegates to IT the responsibility to establish (and implement as needed) procedures to restore any data lost in a disaster. IT has developed the IT Contingency Plan that addresses certain disaster scenarios. The Security Official shall cooperate as necessary with IT to update as necessary the Business Impact Analysis ("BIA") under the Business Continuity Plan.
- c. **Emergency Mode Operation Plan.** The Security Official delegates to IT the responsibility to establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of ePHI

while operating in the emergency mode. IT has developed the IT Contingency Plan that addresses certain disaster scenarios. The Security Official shall cooperate as necessary with IT to develop a Business Impact Analysis which will result in a Business Continuity Plan.

- d. Contingency Plan.** If a disaster, an emergency, or the activation of a contingency plan compromises the integrity or availability of CODA ePHI and IT is unable to restore the ePHI, the Security Official shall request that the institution replace the ePHI.

14. Evaluation

From time to time, the Security Official shall work with IT to perform a technical and nontechnical evaluation based on the CODA HIPAA Compliance Policies and Procedures, to determine whether CODA is meeting the requirements of HIPAA Security. Whenever the Security Official becomes aware of environmental or operational changes that affect the security of CODA's ePHI, the Security Official shall work with IT to perform such an evaluation. The Security Official shall delegate to IT the responsibility to perform security evaluations on systems on a regular basis, and to perform security tests whenever there is a major upgrade to the system.

15. Business Associate Contracts and Other Arrangements

The Security Official may permit a downstream Business Associate to create, receive, maintain, or transmit ePHI on behalf of CODA only if an appropriate Business Associate Agreement has been executed with the downstream Business Associate.

- a. Written Contract or Other Arrangement.**

- (1) Business Associate Agreement.** IT and the Legal Division have developed a Business Associate Agreement that, in general, all downstream Business Associates must execute before they may access PHI or ePHI.

(2) Signing Agreements. The Security Official shall submit a Request for Legal Review of Contract form to Legal for each new downstream Business Associate that CODA is aware of that will have access to PHI. The documents will be executed in accordance with the ADA Signature Authority Policy.

16. Controlling Access to the CODA Facility and Information Systems

a. Facility Security Plan.

(1) Building Security. The Security Official delegates to the ADA building management company the responsibility to develop and implement adequate policies and procedures to safeguard CODA's physical infrastructure at 211 E. Chicago Avenue, Chicago IL. The building management company shall be responsible to:

- (a)** staff the base building (lobby and lower levels) with 24/7 security
- (b)** maintain a building access card system, both for base building and to each specific tenant's space (e.g., ADA employees only have access to ADA offices)
- (c)** maintain building video surveillance which monitors the base building, garage, loading dock, alley, certain portions of the exterior and the 22nd floor.

(2) Access to ePHI through the Building and Equipment. The Security Official shall determine which individuals should be authorized to access the areas of the CODA facility (and the equipment in the CODA facility) that provide access to ePHI. The Security Official delegates to HR and the building management company the responsibility to develop and implement procedures to permit access only to those individuals.

b. Controlling and Validating Access. The Security Official delegates to the building management company the responsibility to implement procedures to control and validate access to facilities by workforce members, visitors, subcontractors (including those who test and revise software programs), and others. The Security Official shall delegate to IT the responsibility to confirm that any individual who is not a workforce member and who requires access to CODA's electronic systems that contain ePHI meets the following conditions:

- (1) a Business Associate Agreement is in place
- (2) the appropriate credentials of the representative of the Business Associate have been verified as appropriate
- (3) Business Associate representative is aware of CODA's security policies and procedures

The Security Official shall train all workforce members to ensure that all ADA computers containing ePHI that are used inside or outside of the facility are password protected. Site visitors will be trained to install full disk encryption software on any computer used to access CODA ePHI.

The Security Official shall delegate to HR and the building management company, as applicable, the responsibility to assign facility keys and alarm system codes to designated CODA workforce members and the responsibility to collect keys and change access authorization when workforce members change jobs or assignments or are terminated.

c. Records of Building Maintenance. The building management company is responsible for documenting repairs and modifications to the physical components of a facility that are related to security (for example, doors and locks).

17. Workstation Use

Each computer that is being used to access CODA ePHI is a “Workstation.” The Security Official shall implement procedures that specify:

- a. What functions may not be performed on a Workstation
- b. How permitted functions must be performed
- c. The appropriate physical surroundings of a Workstation

The Security Official shall set forth these procedures in the Training Manual.

18. Workstation Security

To restrict access to authorized users, the Security Official shall implement physical safeguards for all Workstations. The Security Official shall include such physical safeguards in the Training Manual.

19. Controlling Electronic Devices and Media

CODA shall implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of the CODA facility, and the movement of these items within the facility.

- a. **Disposal.** The Security Official shall delegate to IT the responsibility to dispose of any hardware or electronic media owned by ADA that has been used to access ePHI. IT shall overwrite the hard drive of any de-acquired computers with random data at least three times using a utility called “Autoclave” or a utility called “Secure Data Disposal,” per Department of Defense Standard 5520. IT shall test alternative techniques for data destruction and determine whether to upgrade the pre-disposal data destruction technique.

The Security Official shall include in the Training Manual procedures that workforce members who use computers that are not owned by ADA to access ePHI must follow to thoroughly erase the hard drive prior to de-acquiring any

such computer, using technology specified by IT.

- b. Media Re-Use.** The Security Official shall implement procedures for removal of ePHI from electronic media before the media are made available for re-use. The Security Official shall delegate to IT the responsibility to adequately remove ePHI from electronic media owned by ADA before the media are made available for re-use within the ADA facility. Whenever possible, CDs and DVDs shall be destroyed rather than reused. The Security Official, in cooperation with IT, shall develop and include in the Training Manual procedures and restrictions regarding the use, re-use, and de-acquisition of removable media.
- c. Cleaning Hardware and Media before Reassignment or De-acquisition.** The Security Official shall delegate to IT the responsibility to set standards for electronically cleaning hardware and electronic media that has been used to access ePHI before reassignment or de-acquisition, and to electronically clean such hardware and media owned by ADA. The Security Official shall include in the Training Manual the techniques that workforce members must use to clean hardware and media that is not owned by the ADA before such hardware or media are reassigned or de-acquired.
- d. Replacing ePHI that is Lost due to the Movement of Equipment.** If ePHI is lost when moving equipment, the Security Official shall request that IT replace the lost ePHI through its routine backup or shall request the appropriate institution to resend the ePHI, if necessary for legacy retention purposes.

20. Technical Safeguards to Control Access to ePHI

The Security Official shall implement technical policies and procedures for electronic information systems that maintain ePHI, in order to allow access only to those persons or software programs that have been granted access.

- a. Unique User Identification.** The Security Official shall delegate to IT the responsibility to assign a unique username to each workforce member to identify and track the identity of workforce members using electronic information systems to access ePHI. The Security Official delegates to IT the responsibility to assign a unique user ID to each workforce member authorized to access ePHI using ADA Connect or Knowledge Center. For ADA Connect, IT authorizes the unique user ID access to the ADA Connect system, and the ADA Connect CODA Site Administrator authorizes the unique user ID access to CODA controlled data. For Knowledge Center, IT authorizes the unique user ID to access the system, and CODA staff authorize the unique user ID access to CODA controlled data.
- b. Emergency Access Procedure.** The Security Official shall work with IT, in connection with the Business Impact Analysis, to establish and implement as needed procedures for obtaining necessary ePHI during an emergency.
- c. Automatic Logoff.** The Security Official shall train workforce members to activate a password protected screensaver to automatically logoff after a period of inactivity on any computer used as a Workstation outside of the CODA facility.
- d. Encryption and Decryption.** The Security Official shall train workforce members not to download ePHI onto computers that are not owned by ADA. The Security Official shall, in cooperation with IT, designate acceptable files and transmittal methods and shall include in the Training Manual procedures for transmitting and accessing ePHI. The Security Official shall train workforce members not to use files and transmittal methods that are not approved by IT. The Security Official shall require institutions to e-mail PHI only as an attachment encrypted using a technique that renders the PHI “secure” under the

HIPAA Breach Notification Rule. The Security Official and IT shall determine where it is appropriate to use encryption for electronic transmissions and shall implement a mechanism or procedure to encrypt electronic patient information whenever deemed appropriate.

21. Audit Controls

The Security Official shall implement procedural mechanisms that record and examine activity in information systems that contain or use ePHI as follows: when the Security Official receives a report of unauthorized activity in information systems that contain or use ePHI, he or she shall cooperate with IT to investigate the activity, determine whether unauthorized access to ePHI occurred, and take reasonable measures to prevent harm and to prevent further similar unauthorized access.

22. Authenticating the Integrity of ePHI.

The Security Official shall train workforce members to notify him or her promptly if the workforce member suspects that ePHI has been altered, destroyed, or corrupted. The Security Official shall respond to such a report by requesting that the institution resend an accurate copy of the ePHI.

23. Authenticating the Identity of Persons and Entities.

The Security Official shall implement procedures to verify that a person or entity seeking access to ePHI is the one claimed. The Security Official shall delegate to IT the responsibility to implement technical safeguards requiring that any user seeking access to ePHI possess credentials that authenticate access and to define technical and procedural mechanisms to authenticate the identity of users and/or processes that access CODA electronic systems and ePHI, and to implement procedures to enforce authentication.

24. Security and Integrity of ePHI that is Transmitted Electronically.

The Security Official shall implement technical security measures to guard against unauthorized access to ePHI that is being transmitted by CODA over an electronic communications network. The Security Official shall respond to a report that electronically transmitted ePHI has been altered or destroyed by requesting that the institution resend an accurate copy of the ePHI.

25. If an Institution Violates the Business Associate Agreement.

If the Security Official knows of a pattern of activity or practice of a downstream Business Associate that constitutes a material breach or violation of the entity's obligation under the Business Associate Agreement, the Security Official shall take reasonable steps to cure the breach or end the violation, if feasible. The Security Official shall train workforce members to notify him or her promptly if they discover a pattern of activity or practice of downstream Business Associate that appears to constitute a material breach or violation of the entity's obligations under the Business Associate Agreement.

26. Restrictions on CODA's Use and Disclosure of PHI.

The Business Associate Agreement between CODA and a Covered Entity institution must contain a provision establishing the permitted and required uses and disclosures of that institution's PHI. CODA workforce members shall not use or disclose PHI received from a Covered Entity institution except in compliance with that provision, or as required by law. With two exceptions, the Business Associate Agreement may not authorize CODA to use or further disclose the information in a manner that would violate HIPAA Privacy if done by the Covered Entity. The first exception is that, in certain cases, CODA may use and disclose the PHI for its own management, administration, and legal responsibilities (see paragraph 35) The second exception is that the contract may permit

CODA to provide data aggregation services relating to the Covered Entity's health care operations (health care operations includes accreditation).

27. Duty to Report Uses and Disclosures Not Provided For in the Business

Associate Agreement and Duty to Report Breach of Unsecured PHI.

If CODA becomes aware of any use or disclosure of the PHI that it holds that is not provided for by the applicable Business Associate Agreement between CODA and an institution that is a HIPAA Covered Entity, CODA shall report such use or disclosure to the institution. CODA must also notify a Covered Entity institution of any breach of its unsecured PHI as required by the HIPAA Breach Notification Rule. The Security Official shall train workforce members to report immediately to him or her any suspected unauthorized use or disclosure of PHI, and any suspected breach of unsecured PHI, of which they become aware. Upon receiving any such report, the Security Official shall determine, in consultation with the Legal Division, whether such use or disclosure was provided for in the applicable Business Associate Agreement and whether such use or disclosure constitutes a breach of unsecured PHI. If the Security Official determines that the use or disclosure was not provided for in the applicable Business Associate Agreement, then the Security Official, in consultation with the Legal Division, shall report such use or disclosure to the institution. If the Security Official determines that CODA has discovered a breach of unsecured PHI, the Security Official shall, in consultation with the Legal Division, provide any required notification.

28. CODA's Agents and Subcontractors.

CODA shall ensure that any of its agents, including any subcontractor, to whom it provides PHI received from a Covered Entity, or created or received by CODA on behalf of a Covered Entity, agrees to the same restrictions and conditions that apply to CODA with respect to such information. The Security Official shall notify the ADA Legal Division

of any new agents or subcontractors. The Security Official shall train all workforce members not to disclose PHI to an agent or subcontractor that has not been approved by the Security Official to receive such information.

29. If an Individual Requests Access to PHI.

CODA shall make available PHI to an individual as required by the HIPAA Privacy Rule (45 U.S.C. § 164.514, "Access of Individuals to Protected Health Information"). The Security Official shall train all workforce members to respond to any request from an individual (or an individual's personal representative) to access an individual's records by declining to provide such information and promptly notifying the Security Official of such request. The Security Official will, in consultation with the Legal Division, review any individual's request to access PHI and determine how to respond to the request.

30. If an Individual Asks CODA to Amend PHI.

CODA shall make PHI available for amendment and shall incorporate any required amendments to PHI as required by the HIPAA Privacy Rule (45 U.S.C. §164.526, "Amendment of Protected Health Information").

The Security Official shall train workforce members to notify him or her immediately of any request by an individual to amend either PHI or a record about an individual.

The Security Official shall be responsible, in consultation with the Legal Division, to receive and process such a request. The Security Official must act on such a request within 60 days of receipt. If the Security Official is unable to act on the request within 60 days, the Security Official may obtain one 30-day extension by providing the individual with a written statement of the reasons for the delay and the date on which the Security Official will complete action on the request.

The Security Official will, in consultation with the Legal Division, review any individual's request to amend PHI or a record about an individual and determine how to respond to the request.

31. If an Individual Requests an Accounting of Disclosures

An individual has a right to receive an accounting of disclosures of PHI made in the six years prior to the date on which the accounting is requested, with certain exceptions. The accounting is not required to include disclosures for accreditation purposes, which are considered health care operations as defined by HIPAA. When required, CODA shall make available the information required to provide an accounting of disclosures in accordance with 45 CFR §164.528. Upon receipt of an appropriate request for an accounting of disclosures, the Security Official shall work with the Legal Division to determine the disclosures that must be included in an accounting, and will determine how such an accounting would be generated. The Security Official will train workforce members to notify him or her immediately upon receiving a request for an accounting of disclosures. The Security Official will, in consultation with the Legal Division, respond to a request for an accounting of disclosures.

The Security Official will document the content of each accounting requested, each written accounting provided and maintain the documentation for six years from the date of its creation or the date when it was last in effect, whichever is later. The Security Official will keep a log of paper record disclosures. Electronic disclosures will be tracked by electronically.

32. Making CODA Practices, Books, and Records Available to HHS

To the extent required by law, CODA shall make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by CODA on behalf of a Covered Entity institution available to the Secretary of the U.S.

Department of Health and Human Services (HHS) for purposes of determining compliance with the HIPAA Privacy Rule. The Security Official shall train workforce members to notify him or her immediately upon receipt of any communication from the HHS, the Office for Civil Rights, or a state attorney general. The Security Official, in consultation with the Legal Division, shall be responsible for making such information available in compliance with the HIPAA Privacy Rule.

33. Termination of a Contract with an Institution: Return, Destroy, or Protect the Institution's PHI

At termination of a contract between CODA and a Covered Entity institution, the Security Official shall extend the protections of the Business Associate Agreement to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible, because it may not be feasible to return or destroy such information due to U.S. Department of Education requirements. Upon termination of a contract between CODA and a Covered Entity institution, the Security Official shall determine whether it is feasible to return or destroy all PHI received from the institution, or created or received by CODA on behalf of the institution. If the Security Official determines that such return or destruction is feasible, the Security Official shall return or destroy the PHI, as appropriate. If the Security Official determines that such return or destruction is not feasible, the Security Official shall extend protections of the Business Associate Agreement to the information and limit use and disclosure of the information to the purposes that made its return or destruction infeasible.

34. Termination if CODA Violates the Business Associate Agreement

The Business Associate Agreement between CODA and a Covered Entity institution shall authorize the institution to terminate the contract if it determines that CODA has violated a material term of the contract.

35. CODA's Use and Disclosure of PHI for its Management, Administration, and Legal Responsibilities

The Business Associate Agreement that CODA develops for use with each of the Covered Entity institutions that it accredits shall contain the following provisions:

- a. Use of PHI.** If necessary, CODA may *use* for the following purposes the information that CODA receives in its capacity as a Business Associate:
 - (1)** CODA's proper management and administration; or
 - (2)** To carry out CODA's legal responsibilities
- b. Disclosure of PHI.** CODA may ***disclose*** such information for those purposes if:
 - (1)** The disclosure is required by law, or
 - (2)** CODA obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

36. Safeguards to Prevent Inappropriate Use or Disclosure of PHI.

CODA shall develop and implement appropriate safeguards to prevent unauthorized use or disclosure of PHI in any format, including electronic, oral, or hard copy (such as paper or films) other than as provided for in the Business Associate Agreement between CODA and the Covered Entity institution. The Security Official shall set forth in the Training Manual procedures to safeguard PHI and shall update the Training Manual from time to time as appropriate. The Security Official shall train workforce members to comply with the procedures in the Training Manual. In addition to the safeguards set forth elsewhere in these Policies and Procedures, CODA shall:

- a. Mitigate Harmful Effects of a Wrongful Use or Disclosure.** The Security Official shall mitigate, to the extent practicable, any known harmful effect of a use or disclosure of PHI in violation of its policies and procedures by a CODA workforce member. The Security Official shall train all workforce members promptly to report any privacy complaint and suspected violation of CODA's policies and procedures to the Security Official. The Security Official shall investigate and document any such complaint or report. If the Security Official determines that CODA privacy policies and procedures have been violated, he or she will determine how reasonably to mitigate any known harmful effects of the violation. In the event of a breach of unsecured PHI, the Security Official shall, in consultation with the Legal Division, evaluate the breach and follow requirements of the Breach Notification Rule and policies and procedures for mitigation of harm.
- b. Comply with Required or Permitted Disclosures of PHI.** The Security Official shall consult with the Legal Division prior to using or disclosing PHI for any purpose that is not permitted or required by the Business Associate Agreement to determine whether the use or disclosure is appropriate and whether it requires authorization from an individual.

© 2010-2023 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.