California Dental Association
1201 K Street, Sacramento, CA 95814
888.232.7645 | cda.org

Health Insurance Portability and Accountability Act and the California Medical Information Act

Compliance Implementation Checklist

All California dental practices must comply with patient information privacy and security laws. The federal Health Insurance Portability and Accountability Act (HIPAA) requires "covered entities" to comply with standards for maintaining the confidentiality, integrity and availability of protected health information. "Covered entities" include health care providers, health plans and health care clearinghouses that transmit patient health information electronically for specific transactions.

Unlike HIPAA, California privacy laws apply to all health care providers irrespective of whether a provider transmits patient information electronically. Compliance with the more restrictive element of overlapping laws is required. Many of HIPAA's privacy requirements mirror existing patient privacy rights in California. For an overview of state and federal privacy rules, review *HIPAA and California Health Information Privacy and Protection Laws Q&A* available on cda.org/practicesupport.

A detailed compliance guide is available from the American Dental Association. The ADA Practical Guide to HIPAA Compliance can help a dentist develop or update office policies and procedures. We strongly recommend using the ADA guide with this checklist. The guide has sample forms and policies and provides thorough discussions and considerations on how HIPAA compliance affects a dental practice. Refer to the ADA guide for almost every item listed on this checklist.

Compliance with state and federal privacy laws requires specific recurring actions, plenty of documentation and continual staff training. It is an ongoing process of assessment, implementation and training. This checklist is intended to provide an at-a-glance view of the compliance elements.

HIPAA documentation can be maintained electronically or on paper. All HIPAA-related documents, including policies, training records, employee sanction records, patient authorization for records release forms, risk analysis, risk management plans and much more must be maintained for at least six years. HIPAA is enforced by the U.S. Department of Health & Human Services Office for Civil Rights.

Administrative

☐ **National Provider Identification Number.** Obtain a type 1 (individual) NPI number and, upon becoming a practice owner, a type 2 (organization) NPI number. A dentist may have as many type 2 NPI numbers as the number of practices he or she owns but will only ever have one type 1 NPI number. Even if a dentist is not a HIPAA-covered entity, he or she should obtain a type 1 NPI number. A prescriber must provide a type 1 NPI number in order for a pharmacy to fill a patient's prescription. On claim forms, the type 1 number is used to identify the treating provider and the type 2 number is used to identify the billing entity.

Register and find more information at nppes.cms.hhs.gov/?forward=static.npistart#/.

- ☐ **Privacy and Security Officers.** Designate one person to be both the privacy and security officer for the practice or assign two individuals the different responsibilities. The privacy officer is responsible for implementing privacy policies and procedures and for training staff on them. The privacy officer also may receive and process patient and third-party requests for patient information and for amending information. The privacy officer receives complaints regarding privacy and information requests on the practice's Notice of Privacy Practices. The privacy officer ensures required documentation is completed and retained for specified periods. The security officer shares some responsibilities with the privacy officer with regard to administrative policies and procedures. The security officer's chief responsibility is for the security of patient information that is stored, used and transmitted electronically and may work with outside vendors on the risk analysis, risk management plan and consideration and implementation of administrative, technical and physical security safeguards.
- ☐ **Risk Analysis and Risk Management Plan.** Analyze and assess how patient information is used, managed, stored and transmitted in the practice and consider ways that information may be accessed by unauthorized individuals or unintentionally released. Identify information system vulnerabilities and threats (human, natural, man-made). Risk levels should be assessed periodically and documented. Describe how risk is managed, especially identified high-risk situations. Guidance and a risk assessment tool are available from the following websites:
  - Security Rule Guidance Material
  - HealthIT.gov Privacy and Security
- ☐ **Contingency Plan.** Develop a written plan for situations that can affect the usability and security of patient information, such as a fire, equipment theft, equipment malfunction or a power outage. The plan should include procedures for accessing patient information in an emergency and procedures for accessing the physical location of the computers to restore accessibility to patient information. Refer to the DHHS document Security Standards: Administrative Safeguards for more information on what a contingency plan should include.
- ☐ **Clearinghouse.** If a clearinghouse is used, determine if it is part of a larger organization. If it is, obtain assurances that the clearinghouse has policies and procedures to prevent the larger organization from accessing information without authorization.

Policies and Procedures

Develop and implement written procedures and policies for staff to follow. The policies and procedures address how the dental practice will prevent the unauthorized and unintentional release of protected health information in all forms of communication – oral, written and electronic. Understand what health information is permissible to disclose without patient authorization and under what circumstances.

- ☐ **Privacy Safeguards for Verbal and Written Patient Information.** Describe procedures (safeguards) for ensuring oral communication of patient information is not overheard by others and that written patient information is not viewed by unauthorized individuals, misplaced, or sent to unauthorized individuals via fax or mail.
- ☐ **Patient Access to Records and Right to Accounting of Information Disclosures.** Describe the office procedure for managing a patient's request for records and for responding to a patient's request for an accounting of the practice's disclosures of patient information. Note that California laws are applicable.
- ☐ **Patient Right To Limit Information Use and Disclosures and To Amend Information.** Describe office procedures for managing a patient's request to limit the practice's use and disclosure of patient information to others and to amend his or her record.
- ☐ **Patient Right To Choose How To Receive Communication.** Describe office procedure for managing a patient's request to have practice communications sent through different means or to a different address or telephone number.

- ☐ **Third-Party Access to Patient Information.** Describe office procedure for managing a third-party's request for patient information. Include the "minimum necessary" requirement and note which uses or disclosures require patient authorization. Note that California laws are applicable.
- ☐ **Patient Complaints and Inquiries Regarding Notice of Privacy Practices.** Describe the office procedure for managing a patient's complaint or inquiries regarding the practice's privacy policies. Include the non-retaliation statement. Do not require the waiver of HIPAA rights.
- ☐ **Marketing and Sale of Patient Information.** Describe how the practice may use patient information for marketing purposes and when and how patient authorization is obtained. Document the office policy for selling patient information.
- ☐ **Privacy and Corrective Action policies for the employee manual.** Make employees aware that they will be disciplined for failing to comply with the practice's privacy and security policies and procedures, and that discipline can include termination of employment.
- ☐ **Physical Access and Security.** Describe office procedures to ensure only authorized individuals have access to the practice workstations, servers and any other device that stores or transfers patient information electronically. Describe the functions to be performed on each workstation (including portable devices), the manner in which the functions are to be performed and the physical attributes of the area where specific workstations that can access electronic protected health information are located.
- ☐ **Disposal of Patient Information.** Describe procedures for ensuring that patient information, in electronic form and in charts, radiographs, models and other hard copies, is destroyed or rendered unreadable.
- ☐ **Portable Devices.** Describe how portable electronic devices with patient information are checked out of and into the office, how their physical locations are tracked, and which users are authorized. Address the use of unauthorized portable electronic devices in the practice, e.g., flash drives owned by staff.
- ☐ **Data Backup.** Describe how electronically stored patient information is duplicated, stored and retrieved when needed.
- ☐ **Hardware and Media Tracking.** Describe procedures for tracking the movement of electronic hardware and media that hold patient information both within the office and outside the office.
- ☐ **Hardware and Media Disposal and Re-Use.** Describe how electronic hardware and media that hold patient information are managed to ensure destruction of that information, or to render it unusable, prior to the disposal or re-use of the hardware and media.
- ☐ **Data Breach/Security Incident Response Plan.** Describe office procedures following a breach of unsecured patient information or unauthorized attempt to access patient information. Specify who (privacy officer, security officer or practice owner) takes the lead to notify law enforcement, communicate with the media, draft patient communications, and more. Also, refer to maintenance of a security incidents log. Note that California laws are applicable.

  Review *Data Breach Notification Requirements* on cda.org/practicesupport
- ☐ **Mitigation of Harm.** State policy to lessen the harm of any improper use or disclosure of patient information.

Documents

- ☐ **Notice of Privacy Practices.** Develop this patient notice of your practice's privacy policies and procedures. Post in the practice and on practice website. Make available to anyone upon request. Obtain patient acknowledgement of receipt of notice.
- ☐ **Patient Authorization for Release of Records.** Develop a form or customize the sample form *Patient Request to Access Records (Records Release)* available on cda.org/practicesupport.
- ☐ **Business Associate Agreement.** Enter into agreement with any entity that the dental practice allows to have access to patient information for nonclinical purposes. The agreement is to ensure privacy and security of the information. Ensure business associate agreements made before 2010 have been amended to include the business associate's obligation to comply with the HIPAA Security Rule. Refer to the sample *Business Associate Agreement* on cda.org/practicesupport.
- ☐ **Use or Disclosure Authorization.** A patient must authorize the use or disclosure of his or her information for purposes that are not permitted by law, not considered treatment, payment or business operations (limited by California law), not for public benefit and not legally required.
- ☐ **Communicating Via Unsecure Email.** A patient must authorize the practice to communicate with them via unencrypted email. This authorization should be in writing. It can be a separate form, or language in an email authorizing unsecure communication.

Security

Security Rule guidance material is available on the DHHS website.

- ☐ **Information System Access.** Ensure that access to patient information is provided only to those individuals in your practice and business associates who need the information to perform their job functions. System must be able to recognize individual users, which means unique user passwords are required.
- ☐ **Data Encryption.** Encryption is not specifically required. However, it is strongly recommended to do so because the breach or theft of unencrypted data subjects a dental practice to the cost of notifying patients, as well as to potential fines and penalties.
- ☐ **Transmission Security.** Transmit information electronically in a secure manner, i.e., encryption or use of a secured server.
- ☐ **Facility Repairs and Modifications.** Maintain a record of any repair or modification related to the facility's security system.
- ☐ **System Review.** Periodically (at least weekly) review information system records, such as audit logs, for unauthorized or unusual activity. Periodically test information system security.
- ☐ **Data Integrity.** Take steps to protect data from being altered or damaged and implement process to verify that data has not been altered or damaged.
- ☐ **Malicious Software and Viruses.** Take steps to protect information system from malicious software and viruses.
- ☐ **Security Incidents Log.** Record any unauthorized attempt, successful or not, to access patient information.

Employees

- ☐ **Determine Access Level.** Determine, either by individual employee or job position, the appropriate level of access to patient information necessary to perform job responsibilities. The "minimum necessary" rule applies to employee access to patient information.
- ☐ **Training.** Train employees and others who work in the dental practice (e.g., student interns, independent contractors) on the dental practice's privacy policies and procedures. Obtain acknowledgement of training. Training documentation should include name of trainer, date of training, training subject(s), training resources and participant names. Retrain when policies and procedures change. Retrain when it is clear that policies and procedures are not being followed. Designated security and privacy officers may need a higher level of training.
- ☐ **Employment Termination.** When an employee, independent contractor, or intern is no longer working at the practice, be sure to change or delete access codes or keys to the information system and to the office. Refer to *Decision to Terminate Checklist* on cda.org/practicesupport.