PATIENT RECORDS
Requirements and Best Practices

Both state and federal law regulate the management of patient records and the information contained therein. Federal laws include the Health Insurance Portability and Accountability Act (HIPAA) and its amendments, the most recent of which is the Health Information Technology for Clinical Health (HITECH) Act of 2009. California laws include the Dental Practice Act as well as the Confidentiality of Medical Information Act (CMIA), which subject California health care providers who are not HIPAA covered entities to HIPAA-like requirements with respect to the privacy and security of patient information. Other state laws address patient access to health records, security breach notice requirements, and use of health information for marketing purposes. Information and resources for complying with HIPAA and HITECH are available through *The ADA Practical Guide to HIPAA Compliance: Privacy and Security (2010)*. Links to other resources available on cdacompass.com are listed below.

Format and Content of the Patient Record

The state Dental Practice Act has specific requirements on treatment entries in the patient chart:

> Treatment Entries: Every dentist, dental health profession, or other licensed health professional who performs a service on a patient in a dental office shall identify himself or herself in the patient record by signing his or her name, or an identification number and initials, next to the service performed and shall date those treatment entries in the record. If an identification number system is used, maintain in the practice a master log of all employees' identification numbers. Many offices choose to use dental license numbers as unique identification.
>
> Altering a patient's record with intent to deceive is unprofessional conduct. Correct entries using single-line strikeouts, and note the date the correction was made. Do not use opaque correction fluid or tape. It should be clear that there is no attempt to hide information.

The state further requires that if electronic recordkeeping systems are ***only*** utilized in the dental office, the office must use an offsite backup storage system, an image mechanism that is able to copy signature documents, and a mechanism to ensure that once a record is input, it is unalterable. The dentist must develop and implement policies and procedures to include safeguards for confidentiality and unauthorized access to electronically stored record, authentication by electronic signature keys, and systems maintenance. Original hard copies of patient records may be destroyed once the record has been electronically stored. The printout of the computerized version shall be considered the original.

Liability insurance companies and professional standards of practice dictate best practices to follow for determining what information should be kept in a patient record. The use of SOAP (subjective, objective, assessment, and plan) notes is highly recommended. Subjective notes include patient's description of his or her own health condition and health history. Objective notes include findings from x-rays,

examinations, and tests. Assessment notes include a diagnosis or a list of other possible diagnoses. Plan notes are the recommended treatment or treatment options. Plan notes also can include a summary and outcome of your discussion with the patient.

The CDA-endorsed professional liability insurance company, The Dentists Insurance Company (TDIC) recommends complete records include:

- A description of the patient's original condition
- Your diagnosis and treatment plan
- Progress notes on the treatment performed and the result of that treatment
- Patient's personal information
- Medical history (all questions answered) and regular updates
- Oral cancer screening and TMJ evaluation
- Diagnostic test findings and exam notes
- Consultant reports, reports to and from specialists and physicians
- Notes objectively describing complaints or confrontations
- Notes about rescheduled, missed or canceled appointments
- Exam and treatment notes
- Informed consent conversations and forms
- Models
- All radiographs taken at intervals appropriate to the patient's condition
- Correspondence to/from the patient inclusive of phone calls, e-mails, voice messages, letters and face-to-face conversations

The outside cover of a chart should display only the patient's name and/or account number. A color-coded system is recommended if clinical staff think it necessary to have a method to alert them to a patient's health status that will affect dental treatment. For example, a colored sticker on the outside front of the folder can prompt the dentist or hygienist to look more closely at a patient's chart.

Patient Access to Record

A patient record can include any written document in the chart, even if it is non-clinical, x-rays, photographs, and models. Access to patient records may not be withheld due to an unpaid bill for healthcare services.

Inspection: Upon presentation of a written request, a patient or patient's representative has the right to inspect the patient's records. The inspection of the records should take place during business hours and within five (5) working days of receiving the written request. It is advisable to have an office employee present in the room when the patient or patient's representative inspects the record.

Paper Copy: A patient or patient's representative is also entitled to receive a copy of the record once a written request is presented to the office. The dental office should provide all copies within 15 days of receiving the written request. A patient of a HIPAA-covered entity is entitled to a copy of the record, even if a copy has been provided to another healthcare provider at the patient's request. ***Allowable charges***: A HIPAA-covered entity may not ask payment for costs incurred in locating and making the records available. The dental office may collect from the patient no more than 25 cents per page, or 50

cents per page for copies made from microfilm. All reasonable costs, not exceeding actual costs, incurred by the dental office to provide the copies may be charged to the patient. This includes the cost of copying x-rays and postage if the patient requests receipt by mail.

Electronic Copy: If a dental practice maintains a patient's record in electronic form, the patient may receive, upon written request, an electronic copy of the record and may direct the dental practice to transmit an electronic copy to another individual or entity. A patient of a HIPAA-covered entity is entitled to a copy of the record, even if a copy has been provided to another healthcare provider at the patient's request. ***Allowable charges:*** The fee charged for this electronic copy may not exceed the actual labor costs of fulfilling the request. Regulations with compliance specifics (for example, defining what an acceptable electronic format is and what costs are reimbursable in providing an electronic copy) are pending.

Summary of the Record: State law allows a healthcare provider the discretion to give a summary of the patient's records to a patient requesting a copy of the record. However, a dental practice that is a HIPAA-covered entity may prepare a summary of the patient's record ***only if*** the patient has approved the action in advance. A summary of the record shall be made available to the patient within 10 working days from the date of the patient's request. More time may be allowed to prepare the summary if the record is large, but the summary must be provided within 30 days of the request. ***Allowable charges:*** The dentist may charge no more than a reasonable fee based on actual time and cost for the preparation of the summary.

Public Benefit Program Appeal: If a patient requires a copy of a portion of his or her record to support an appeal regarding eligibility for a public benefit program, such as DentiCal, the copy shall be provided by the dental office at no charge. ***Allowable charges:*** The patient is entitled to no more than one copy free of charge, but may not be limited in the number of requests for copies.

Patient Requests to Amend Record

Both HIPAA and state law provide patients the right to request amendments to their records. However, the laws differ in how a health care provider can respond to such a request. Ideally, a discussion with the patient regarding an amendment should be done prior to initiation of the amendment process. Once a written request for amendment is submitted, the dentist must respond.

California law simply allows a patient to add a statement to the record. A patient amendment can be no longer than 250 words for each item that is believed to be incomplete or inaccurate. The health care provider must include a patient amendment in the record. Except for an emancipated minor, a minor patient does not have the right to amend his or her record.

Under HIPAA, a patient submits a request to the covered entity to amend the record. The health care provider can require a written request be submitted and that the patient provide a reason for the amendment. The provider should respond within 60 days of receiving the request but may have another 30 days if the extension is requested in advance from the patient.

When the patient's request is granted, notify the patient in writing of the decision. Make the amendment to the record without destroying previously entered information. Add notations regarding date of amendment and rationale. Provide amended information to entities identified by the patient and others who the provider knows have legitimate need for the information.

A provider can deny a patient's request only under these circumstances:

- The information proposed to be amended is accurate and complete;

- The information may not be accessed by the patient;
- The information was not created by the provider (unless the provider knows the original provider of the information is no longer available; and
- The information is not part of the patient record.

When the patient's request is denied, notify the patient in writing of the decision. Include in the notification the reason for denial and an explanation of the patient's right to submit a written statement regarding the provider's denial. The patient also must be informed of other rights, including the right to file a complaint with the U.S. Department of Health and Human Services. For additional information, sample policies and forms, refer to *The ADA Practical Guide to HIPAA Compliance: Privacy and Security Kit (2010)*.

Under both federal and state law, information may not be removed from a patient's record under any circumstance. Corrections can be done using single-line strikeouts, and the date the correction was made should be noted. Do not use opaque correction fluid or tape. It should be clear that there is no attempt to hide information

Upon A Dentist's Death or Incapacitation

A dentist, who has been contracted by the estate or trust of a dentist who has died or become incapacitated, shall obtain a form signed by the deceased or incapacitated dentist's patient, or the patient's legal guardian, that releases the patient's dental records to the contracting dentist or dentists prior to use of those records. (B&P 1625.4)

Access to Records by Other Entities

Records can be released to anyone the patient chooses as long as the dental office receives written authorization signed by the patient or the patient's representative and if the dentist has determined that releasing the records will not cause harm to the patient. The authorization form should specify who is to receive the records and if the release of records or information is limited in any way. Restricted and confidential health information with regard to pregnancy, HIV test results, sexually transmitted diseases, mental health, and alcohol or drug abuse may not be provided to a requestor without specific consent from the patient.

If, however, the patient is not the one requesting the information or records, whether the dental office can provide it depends on whom the requestor is and why the request was made. If deciding that a requestor can have information, you are then responsible for determining whether HIPAA's "minimum necessary" rule applies.

Other Health Care Professionals: HIPAA and California law allow a dental practice to provide patient information, without patient authorization, to other health care professionals as long as the purpose of the information is to provide patient treatment.

Although the HIPAA Privacy Rule allows the use and transfer of patient information to relevant parties who need that information for healthcare operations, which includes practice sales, state law does not include the same provision. In the transfer, sale, merger or consolidation of a dental practice, it is therefore prudent for the selling dentist to obtain written patient authorization prior to allowing a potential buyer or partner to view charts. The absent provision in state law also means that a new practice owner should stay on the safe side of the state's privacy laws and obtain written patient authorization before

using a patient record. If a patient sets an appointment to be seen by the new owner, this is viewed as an implied authorization that allows the dentist to view the record before the patient presents. Patient authorization must be separate from the acknowledgement of the office's Notice of Privacy Practices. The authorization form can be mailed to patients together with the selling dentist's notification of transferring practice ownership.

In the transfer, sale, merger or consolidation of a dental practice, the new owner may agree to have custody of the patient record (the alternative is that the former owner retains the records). As the custodian of records, the owner is legally responsible for ensuring the contents are secure and, if the records are to be destroyed, ensuring the contents are unreadable.

Patient's Employer: Employers, in general, do not have the right to access the information except in workers' compensation cases or when necessary to carry out their responsibilities for workplace medical surveillance under Cal-OSHA or similar federal or state laws. Employers who self-insure may have limited access to patient information necessary to determine payment. Employer-sponsored dental benefit plans also have limited access to patient information necessary to determine payment and to conduct quality assessment audits.

Payer: If an individual other than the patient is responsible for paying the patient's bill, disclosure of patient information is allowed as long as the disclosures are limited to the minimum amount of information necessary to obtain payment. In making such disclosures, health care providers also must honor any reasonable request for confidential communication and any agreed-to-restrictions on the use or disclosure of the patients' protected health information. The dental office's Notice of Privacy Practices can state that if a patient designates another person as responsible for payment, the office will disclose the minimum amount of personal health information necessary to obtain payment from that person. If the patient objects to that disclosure, the office should inform the patient that he or she would have to choose between allowing the office to disclose information in order to obtain payment or paying for the services himself or herself. If a patient has paid the full cost of an item or service out-of-pocket and requests that the personal health information regarding the item or service not be disclosed to a health plan for purposes of payment or health care operations, the dental office must honor the patient's request.

Parents -- Divorced or Separated: A parent generally has a right to access the health record of his or her minor child irrespective of whether the parent has custody or financial responsibility. A dental practice may refuse to give access to a parent if it determines that providing access may harm the patient. A parent does not have a right to access the health record of an emancipated minor. An emancipated minor is an individual under 18 yrs old and is either (a) married or divorced; (b) is on active duty with the US armed forces; or (c) received a declaration of emancipation from the court.

Associate: A dentist who is a former associate in a dental practice may not copy or otherwise use patient health information from that dental practice without first obtaining written authorization from the patient.

Mandated Reporting: The obligation of a licensed dental professional to disclose possible domestic abuse, criminal activity, and other legal violations involving patients to appropriate agencies is not hindered in any way by HIPAA or California law.

Representative of Deceased Patient: A legally designated representative or beneficiary of a deceased patient may inspect or obtain a copy of the patient's record. The representative or beneficiary also may grant third-party access to the record. The dental office should request verification of the requestor's status as a deceased patient's representative or beneficiary. A proposed HIPAA rule would allow a dentist discretion to release information to a family member or individual who is involved in the patient's care or with payment for care.

Research Entities and Public Health Organizations: These groups may have limited access to protected health information. Details can be found in *The ADA Practical Guide to HIPAA Compliance: Privacy and Security Kit (2010)*.

Dental Board and DentiCal/MediCal: The Dental Board has the authority to inspect or copy patient records. Representatives of the state Department of Health Care Services, the state Attorney General's Office and the U.S. Department of Health and Human Services have the authority to inspect or copy records of patients whose care is provided through the DentiCal/MediCal program. Neither HIPAA nor CMIA limit the agencies' access to records.

Coroner: California law requires healthcare providers provide information upon a coroner's request to help identify the deceased, locate next of kin, or investigate deaths that may involve public health concerns, organ or tissue donation, child or elder abuse, suicide, poisoning, accident, sudden infant death, suspicious deaths, unknown deaths or criminal deaths.

Law Enforcement without a Subpoena: Sometimes law enforcement will request a health care provider make available protected health information. Although it is prudent to insist upon a subpoena, HIPAA does allow a dentist, without patient authorization, to release protected health information to law enforcement under the following circumstances:

- To report injuries resulting from criminal acts or deadly weapons;
- To respond to court orders, search warrants, court-issued subpoenas, or regulatory agency order;
- To respond to requests for information to identify or locate suspects, fugitives, witnesses, or missing persons;
- To respond to requests for information about a crime victim;
- To alert law enforcement of a suspicious death; and
- To provide evidence of criminal conduct.

Before providing the requested information, verify the identity and credentials of the individual receiving it.

Subpoenas: If a dental office receives a subpoena for a patient's record, circumstances will dictate the way to respond.

If law enforcement serves the subpoena, consult your attorney immediately. Provide the officers with access to the record while informing them that you are contacting your attorney. Do not try to impede law enforcement's access to records.

In many cases, receipt of a subpoena likely arises out of a civil lawsuit. Upon receipt of a subpoena in these cases, evaluate whether you can comply with the demand for records. Consider these questions:

- ***Do you have the requested records?*** If not, provide a statement that you do not have the records.

- ***Is the subpoena issued part of a civil action in California?*** Out-of-state subpoenas are not enforceable in California, except for subpoenas issued in federal cases. Subpoenas issued as part of state administrative hearings or court proceedings have patient notification requirements. Consult with your attorney for more information.

- ***Are you a party to the lawsuit?*** If yes, contact your professional liability carrier.

- ***Is the subpoena valid?*** A subpoena is valid if

  (1) it is personally served on you or someone authorized by you to receive a subpoena;

  (2) it is issued by the clerk of the court or attorney handling the lawsuit;

  (3) it is addressed to you or someone qualified to certify the requested records;

  (4) it contains a date specified for production of records that is at least 20 days after the subpoena was issued and at least 15 days after it was served on you and at least 20 days after notice of the subpoena was received;

  (5) it specifies each item or category of items to be produced; and

  (6) it must have documentation demonstrating that the patient either has consented to the release of records or has been informed of the records request.

The 20 days is specified because time is allowed for the court to hear motions to suppress the subpoena. If the subpoena is valid and you are not a party to the lawsuit, produce the records as requested, sign the affidavit and submit statement for costs incurred in responding to the subpoena.

Marketing Activity: HIPAA limits the use of protected health information for marketing activities on behalf of a covered entity or a third party. California law prohibits solicitation of an individual's health information for direct marketing purposes unless the solicitor informs the individual of the intended uses of the information and obtains the individual's permission. Refer to the article "Dental Practice Marketing" on cdacompass.com.

Patient's Right to Know about Disclosures

A patient has the right to receive an accounting of disclosures of personal health information by healthcare providers who are HIPAA covered entities. It must be provided within 60 days of the request, although the patient may grant, upon request and given reason for delay, an extension of up to 30 days. No fee can be charged for the first disclosure accounting log in a 12-month period. If it is so stated in the dental office's Notice of Privacy Practices, a reasonable fee can be charged for subsequent disclosure accounting logs requested for the same 12-month period. The subsequent disclosure accounting log can be provided after the fee is paid.

The contents of a disclosure accounting log should contain the following elements:

- Disclosure date
- Name and contact information of entity receiving information
- Description of information disclosed
- Purpose of disclosure or copy of the request; and
- If there are multiple disclosures to the same entity of the same type of information, the frequency of disclosures during the accounting period and the date of the last disclosure.

A patient's right to an accounting may be suspended for one of two reasons – belief that the patient may be endangered (e.g., domestic violence situation) or upon request by law enforcement.

The HITECH Act expanded disclosure accounting rules to include HIPAA business associates. In addition, covered entities who maintain electronic health records (EHRs) are now required to provide an accounting of more types of disclosures than covered entities who do not use EHRs. However, the Department of Health and Human Services has not yet adopted regulations implementing this law so the specifics of the accounting log and the implementation date are unknown at this time

Disclosure accounting logs, names and titles of individuals in the dental practice response for receiving and processing requests for disclosure accountings must be retained for six years. For sample forms and more information on accounting of disclosures, refer to *The ADA Practical Guide to HIPAA Compliance: Privacy and Security Kit (2010)*. Your office policies and procedures should describe how you would manage patient requests for accounting of disclosures.

Data Breach Notification Requirement

A healthcare provider is required to notify patients when an actual or suspected breach of personal health and/or financial information has occurred. For information, refer to "Data Breach Notification Requirements Checklist" on cdacompass.com. A sample notification letter also is available on the Web site.

Record Retention & Disposal

State law does not define the period for which a dentist must maintain patient records after the patient discontinues treatment with the dentist. Records of unemancipated minors shall be kept at least one year after the minor has reached the age of 18 years, and in any case, not less than seven years. It is best for you to contact your professional liability carrier for its recommendation. Ideally, all dental records, active and inactive, should be maintained indefinitely. Records must be kept for seven years after a dental practice ceases operations.

Maintain all parts of the record, including radiographs and models. If onsite storage of the inactive patients' charts is not an option, store records offsite in a secured location. Another option is to store records electronically. A patient who has not returned for treatment within the last 24-36 months is inactive. Separate files of inactive adult patients from files of inactive minor patients, as of last treatment date.

Records should be shredded, or disposed in a manner that makes personal information unreadable or indecipherable. Failure or negligence to destroy patient records in a manner that fails to preserve the confidentiality of personal information is a violation of state law. Persons injured because of a dentist's abandonment of patient records may bring action in court against the licensee, or partnership or corporation if applicable.

If hiring a records disposal company, it is recommended to choose one that specializes in destroying records by burning or shredding. Radiographs should be separated from the paper files and, due to the silver content on the film, disposed through a silver recycler, hazardous waste vendor, or household hazardous waste program that accepts small business hazardous waste. A log should be kept of which records are destroyed and when. The log will assist you in identifying which records have been destroyed and are available in the event they are requested later.

Transferring Records in a Sale

If you are selling or transferring your practice, be sure to address two things: (1) transfer responsibility and liability for proper storage and disposal of records to the new practice owner and (2) ensure your continued access to those records for an indefinite period for the purpose of responding to any litigation.

References

Business and Professions Code §§ 1680(s), 1683, 1684.1
California Civil Code Section 56.10 – 56.16
Health & Safety Code §§123100-123149.5, 130200 - 130205
Health Information Technology for Clinical Health (HITECH) Act

Also available on cdacompass.com:

- Health Information Portability and Accountability Act (HIPAA) – An Overview
- HIPAA Security Rule – An Overview
- HIPAA and California Health Information Privacy and Protection Laws Q&A
- HITECH Act Revises Certain HIPAA Provisions
- Data Breach Notification Requirements Checklist
- Dental Practice Marketing

Updated June 2011