Dentist's Advantage
PROFESSIONAL LIABILITY & PRACTICE PROTECTION

The National Society of Dental Practitioners and the Dentist's Advantage Insurance Program for Dentists

RISK MANAGEMENT ARTICLE

Quality Records Protect Dentists in Case of Litigation

The vast majority of dentists function at a high level, providing quality care that results in positive outcomes for patients. As you well know, however, not every outcome will be a positive one, and at times a patient who is unhappy with the results will take legal action. In a malpractice case, inadequate dental records can hamper the attorney's efforts to resolve a complaint in your favor. You can be positively protected if you are creating and maintaining proper dental records by following the guidelines in this article.

Reasons for recordkeeping

Protection against litigation is not the only reason accurate records are essential. At the most basic level, a good dental record promotes quality of care by providing a roadmap of all that has happened to the patient. This roadmap can also be read by consulting dentists and by another dentist should the patient change practices.

A more somber reason for keeping records is the occasional need to provide information to a forensic dentist so a postmortem identification can be made. In some cases, positive identification is of significant help to family members who may have been living with uncertainty for months or even years.

Rules and regulations

Some states outline specific requirements for dental records, but more commonly, requirements are found in laws and regulations related to patient care in general. Review your state dental practice act, which is usually available online, and consult your state dentistry board for information.

You also need to consider the HIPAA Privacy Rule (modifications to the rule effective 2002) and Security Rule (effective 2003). The Privacy Rule applies to health information in any form, while the Security Rule covers electronic protected health information that is created, received, maintained, or transmitted. The Security Rule requires safeguards for protecting confidentiality (nondisclosure of information to unauthorized persons), integrity (data is not changed without authorization), and availability (authorized individuals can access information) of electronic patient information.

The 2013 HIPAA Privacy and Security Omnibus Rule strengthens these rules and extends them to dental practices' business associates (e.g., billing services, a document storage company) and their contractors. The Omnibus Rule also slightly modified the Breach Notification Rule of the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act. In essence, breach notification requires dentists to notify affected patients, the federal government, and in some instances, the media if a breach in secure information occurs. In addition to laws and regulations, the American Dental Association (ADA) Principles of Ethics and Code of Professional Conduct addresses dental records, noting that dentists are "obligated" to keep records confidential.

Contents of the dental record

The ADA recommends keeping financial information, such as invoices, insurance claims, and payments, separate from the clinical record. The clinical record, which is the focus of this article, should contain all the information needed to develop an effective treatment plan(s), monitor progress, and ensure continuity of care (see *Contents of the dental record*).

Dentist's Advantage
PROFESSIONAL LIABILITY & PRACTICE PROTECTION

The National Society of Dental Practitioners and the Dentist's Advantage Insurance Program for Dentists

RISK MANAGEMENT ARTICLE

Ensure that staff members understand the importance of keeping the dental record current and confidential. Both dentists and staff members also need to follow basic documentation principles (see *Documentation guidelines*) as all entries must be clear, concise, and accurate.

Records access and transfer

You should have a policy that outlines who has access to records, and the policy should be congruent with HIPAA rules. Dental records should be kept in a secure location, and electronic-based records should be protected through security that includes passwords, which are changed at least quarterly, for those accessing the data.

The HIPAA Security Rule requires periodic risk assessments, staff education, and ongoing maintenance of safeguards. Document your efforts in these areas.

Before releasing any paper or electronic health information, you should obtain permission from the patient per state law and HIPAA requirements. (Some states require patients to give consent before information is released to another healthcare provider.) Send only copies of paper records, retain the originals, and send the minimum amount of information necessary. Keep in mind that according to the ADA Code of Ethics, whether the patient's account is paid should not influence the release of records that are important for future treatment. Note in the patient's record the date, what information was sent, and to whom it was sent. Finally, have outside companies such as a billing service or the vendor for an electronic health record sign agreements that they will adhere to HIPAA regulations.

Records retention and destruction

State laws and regulations typically specify how long records must be retained after the last patient visit. Usually the length of time is longer for children because records are kept for a set time after the child reaches adulthood. HIPAA administrative simplification rules require retention of records that contain protected health information for 6 years after the last visit. This rule preempts state laws that might require a shorter time. Some experts recommend as long as 10 years. The Centers for Medicare & Medicaid Services requires cost report records to be kept for at least 5 years after closure of the report. Consult your professional liability insurer for recommendations in this area. You can access a list of states with links to their medical records information at www.healthinfolaw.org/topics/60 and a list of suggestions for length of time to retain financial information at http://managemypractice.com/recordretention-medical-practices-medical-records-documents. In most cases, accounting records such as bank statements should be kept for 7 years.

You should also have a records retention policy that you communicate to your staff. In the situation of a multi-dental practice or an independent contractor, practice agreements or contracts should spell out who owns the records so responsibility is clear.

If in-office storage becomes an issue, you may choose to use a secure off-storage site or convert to digital. Before doing so, consult with an attorney and your professional liability insurer. Regular backup of records is also essential, including offsite backup such as to a secure cloud.

Take great care when deciding when to destroy inactive records, that is, records that have passed the statute of limitation. First, check state laws to determine if destruction is permissible.

RISK MANAGEMENT ARTICLE

HIPAA privacy and security regulations do not require a particular disposal method for either print or electronic records with protected health information, but does provide examples. In the case of print documents, it recommends "shredding, burning, pulping, or pulverizing" the records. You might want to consider using a professional shredding service. Have the service sign a confidentiality agreement so there is still protection for the information that falls under HIPAA requirements. Ask for a certificate of destruction to keep on file.

Suggestions for disposing of electronic files include "clearing (using software or hardware products to overwrite media with nonsensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media (disintegration, pulverization, melting, incinerating, or shredding)."

Contents of the dental record

Here are some examples of items typically included in a patient's clinical dental record:

- patient identification data such as name, address, email, and employer registration form
- medical (including medications) and dental history information, including updates
- HIPAA acknowledgment form, consent forms, and other waivers or authorizations
- clinical chart of oral conditions
- diagnostic and laboratory test results, as well as radiographs
- treatment plan(s)
- treatment and progress notes
- prescriptions
- consultation and referrals made and the subsequent reports
- record of conversations (including those by phone or electronic transmission) with the patient about treatment plan(s), complaints, patient education, noncompliance, and other key issues; document if the patient declines treatment and if appointments are missed
- nonfinancial-related correspondence to the patient.

Sources: American Dental Association. Dental records. 2010. Kaweckyj N, Frye W, Hilling L, Lovering L, Schmitt L, Leeuw W. The business of dentistry: Patient records and records management. November 21, 2011.

Documentation guidelines

Following these guidelines helps ensure information is communicated accurately and lays the foundation for defense in a court of law.

- Use only standard abbreviations.
- Use the same dentition numbering system, such as The Universal Numbering System, and the same colors and symbols for various conditions in the patient's mouth (such as restorative material) for all patients.
- Sign and date each entry.
- To correct an error on a paper document, cross out the error, insert the correct information, and initial the entry.
- Chart during the patient's appointment (for example, enter the results of a heath history into the electronic record as the patient responds to questions) or immediately after to promote accuracy.
- Don't leave blank lines in between entries when using paper documentation.
- Keep entries objective

Dentist's Advantage
PROFESSIONAL LIABILITY & PRACTICE PROTECTION

The National Society of Dental Practitioners and the Dentist's Advantage Insurance Program for Dentists

RISK MANAGEMENT ARTICLE

Accurate records yield benefits

Dental records support quality care by ensuring key information is readily available for the dentist and those the dentist consults. Accurate records are particularly key to protect you in the case of legal action.

RESOURCES

American Dental Association. Dental records. 2010.
American Dental Association. Principles of Ethics and Code of Professional Conduct. 2012.
American Dental Association. HIPAA Privacy and Security. http://www.ada.org/en/member-center/member-benefits/practice-resources/dental-informatics/electronic-health-records/health-system-reform-resources/hipaa-privacy-security.
Charangowda BK. Dental records: an overview. *J Forensic Dental* Sci. 2010;2(1):5-10.
Kaweckyj N, Frye W, Hilling L, Lovering L, Schmitt L, Leeuw W. The business of dentistry: patient records and records management. November 21, 2011. http://www.dentalcare.com/media/en-US/education/ce390/ce390.pdf.
Medical records retention and media formats for medical records. MLN Matters. n.d.
http://www.cms.gov/MLNMattersArticles/downloads/SE1022.pdf
U.S. Department of Health and Human Services: Office for Civil Rights. The HIPAA privacy and security rules: frequently asked questions about the disposal of protected health information. n.d. http://www.hhs.gov/ocr/privacy/
hipaa/enforcement/examples/disposalfaqs.pdf.
Whaley MP. Record retention for medical practices — medical records and other documents. Manage My Practice. June 29, 2014.
http://managemypractice.com/record-retention-medical-practices-medical-records-documents/.
Accessed Aug. 25, 2014.

Article reviewed by Dr. Kenneth W.M. Judy, DDS, FACD, FICD, PhD
Article by: Cynthia Saver, MS, RN, President, CLS Development, Columbia, Maryland