CNA

# CNA HealthPro

## The Paperless Record

One of the most significant changes in healthcare over the past decade has been the increasing ability to move toward a "paperless" practice. What began with relatively simple billing and financial bookkeeping programs has evolved into integrated patient record and practice management systems with a wide range of capabilities, such as electronic scheduling, clinical progress notes and diagnostic imaging. In fact, many hospitals at the cutting edge of the technology curve have already converted their patient charts to entirely computer-based systems in an effort to reduce communication and medication errors.

Computerized dental record systems have revolutionized the storage of patient information. The systems have the ability to:

- organize all patient information in one place, vastly increasing the data's usefulness, flexibility and accessibility

- save time and space by eliminating the need to pull, refile and store paper files

- facilitate better patient communication by linking digitized radiographs and intraoral camera images with text and by documenting the patient's progress

And from a risk management perspective, certain aspects of electronic patient records are advantageous in comparison to paper charts. Computer records are

- recoverable. Unlike paper records, which can be destroyed in a fire and lost forever, electronic files that have been backed up and stored off-site can be reloaded onto your computer.

- accessible from many locations. By using a modem, a dentist can call up a chart from a home computer to document a phone conversation, or send complete records instantly to similarly equipped consulting dentists.

- consistently legible. Electronically printed records reduce the risk of miscommunication or disputed entries. A legible, complete record is an important shield against malpractice claims.

Electronic systems also allow for more consistent follow-up by automatically reminding office staff to monitor patients' progress. Computers can make the reminder process easier and more reliable by tracking all appointments and printing out reminder letters with a couple of keystrokes.

Whether you are already paperless or are considering a move in that direction, the issues discussed below should help you address any concerns that may arise.

### Viability of Computer Records

The admissibility of computer-based patient records in legal proceedings has been established in numerous healthcare malpractice cases. Additionally, we are not aware of any state board of dentistry that has mandated that dental records be written by hand. For example, the Illinois Dental Practice Act (Section 50, Patient Records) declares

> "Every dentist shall make a record of all dental work performed for each patient. The record shall be made in a manner and in sufficient detail that it may be used for identification purposes." (225 ILCS 25/50)

Clearly, a computerized patient record may be created to fulfill the above criteria. Such records can easily be printed to comply with record requests or referral needs. Should the record become part of the defense of a malpractice claim or dental board complaint, the dentist would simply be required to attest that the printout represents a true and accurate account of the patient's treatment. Our experience indicates that the *format* of the patient record – paper versus electronic – is insignificant relative to the information contained in or missing from the record.

One drawback to many electronic systems is their inability to capture patient signatures on important documents, such as medical histories and informed consents. To overcome this problem, you can either

- **have the patient sign a paper form,** then scan the form into your computer system; or

- **capture signatures on an electronic signature pad,** comparable to credit purchase procedures at certain retail establishments

If you select the first option, retain the original form, as courts prefer original signed documents to copies or other reproductions. You can then archive all original documents alphabetically in a master file, as opposed to creating separate patient charts with each containing only a few pages. This precludes a totally paperless office. However, in today's litigious society, original documentation of the patient's medical history and informed consent represents a critical risk management strategy.

## Record Integrity

A potential pitfall of electronic records is that plaintiff's attorneys may attack the credibility of computer records, asserting that they may have been altered without detection. Record access and security concerns are being addressed through the development of more sophisticated tools. The use of a system that creates audit trails indicating when a record was last modified, coupled with various back-up methodologies that preclude alteration of the note or original digital radiography image can address the issues of access and security.

Almost all changes to a computer record or image are detectable. Although the computer screen appears to contain seamless information, data entered at different times is usually recorded in different locations on the storage media. The varying locations are evidence that data was entered at different times. *Adulteration of computerized records is therefore very easy to detect.* For ethical and legal reasons, no record of any kind should be falsified under any circumstances.

We recommend that dentists using digital radiography retain, in unaltered form, all original images as well as all manipulated images used for diagnostic or treatment purposes. This includes images that have been magnified, field-reversed or contrast-adjusted to better evaluate the patient's condition. Many systems place a marker or icon on any image that has been altered from its original form, making the identification of manipulated images relatively simple.

We also recommend that every person making progress note entries be required to type in his or her name at the end of each note. Dentists should review and electronically "co-sign" staff progress notes by typing their own name after that of the staff member. These steps are necessary to ensure an accurate trail of information and activity.

Even clinical records systems with two protection levels – an initial entry password and a signature password that "stamps" date and authorship on every treatment entry – can be easily and inadvertently breached. The most common occurrence is when one person logs onto a terminal in an operatory or at the reception desk and is then called away, allowing someone else access to the system. This "cross-contamination" of the computer system makes the logon ID essentially worthless in identifying the person posting the entry.

## Record Security

Even if you still have paper charts and use your computer system only for billing purposes, steps must be taken to protect against unauthorized entries and other breaches of patient confidentiality. Potential intrusions range in sophistication from network "hackers" to a nosy patient's casual glance at a poorly located computer screen. The quality of the software and the location of computers are crucial to maintaining security.

Access to confidential information should be password protected, limited to specific portions of the patient record or subject to review by an authorized staff member. Choose obscure passwords and change them regularly. Passwords should be written and stored in a safe deposit box or other secure location.

Computers may be powerful tools, but they're neither foolproof nor immune to accidents and sabotage. These tips can help you protect your electronic records system:

- Be careful with your computer's hard drive. These devices are sensitive to bumps, falls and voltage surges. Always use a surge protector.

- Keep magnets away from your computer and all storage disks and tapes. Magnets can alter or erase electronic storage media.

- Do not surf the Internet with your office computer. The risk of "infection" by a computer virus is too great. If you must have Internet access at the office, set up a stand-alone workstation where you can download any needed information to disks. Then use a virus detection program to check the disk for viruses before uploading the files onto your main system.

## Infection Control

One of the criticisms of paper records is their potential as fomites for infection. All too often, dental personnel handle the folders, papers or radiographs of patient charts without removing soiled exam gloves, cross-contaminating them with pathogens from the patient's mouth.

Computer terminals also must be handled carefully to minimize the threat of infection. A gloved hand can contaminate the keyboard and mouse of an operatory workstation, allowing bacteria to be passed from one patient to another, or to the dentist or staff member who next uses the terminal without gloves. At the front desk, an ill receptionist may pass that illness to other staff members via a shared keyboard or mouse.

To prevent the spread of germs, it is necessary to apply standard infection control measures to operatory computer terminals. Always take your gloves off and wash your hands before using the keyboard. Alternatively, some dentists place plastic protective covers on the keyboard to protect against dust and water spray, then overlay it with a disposable plastic film, which acts as a physical barrier to cross-contamination. Disposable plastic shields can also be used on the mouse. Ask your computer manufacturer which disinfectants are safe to use on your components.

## Record Retention

Record storage and retention are essential aspects of dental practice, whether the patient is in the midst of care or has moved on to another practice. Paper and electronic records alike must be maintained, primarily for treatment continuity but also for risk management purposes.

Most states have record retention statutes, although some do not address the issue of dental record retention. We recommend that records be kept forever whenever possible. On a more realistic level, records should be kept well beyond any point of legal and/or administrative exposure for the dentist. However, the administrative rules for record retention as well as the legal statutes of limitations for malpractice claims vary from state to state. For example, in Illinois, the statute of limitations for adults is two years from the time a reasonable person discovered the injury and no more than four years from the date of injury. Yet, the state dental practice act mandates that records be kept a minimum of 10 years from the last date of treatment.

In many states, the statute of limitations for minor children doesn't begin until they reach the age of majority, usually 18 years of age. A child may, therefore, bring a claim within 18 years plus the two, three or four years accorded by the applicable state statute of limitations. A dentist who discarded the child's records after 10 years would find his or her legal position difficult to defend if a claim were filed after that time.

Consequently, the most prudent course is to retain your records forever. Any shorter time frame depends on state laws. In *most* states, 12 to 15 years for adult records is sufficient.

Consider that time frame in terms of your current patient volume, expected new patients and the amount of information that must be stored in your system, including progress notes, digital radiographs, clinical photographs, predictive images and treatment mockups.

Clearly, if you adopt a paperless record system, you'll need a great deal of electronic storage capacity going forward as well as the ability to access that stored information. When selecting software, consider the long-term viability of the vendor, potential obsolescence of the program and compatibility with any software you currently use.

## Backing up Your Records

Back up your computer data every day and store the backup data away from the office each night to prevent a total loss of data in the event of a power surge, burglary, fire, flood or other catastrophic event. No hard drive lasts forever, so constant backup is necessary to maintain the continuity and integrity of a computerized record system should a problem arise.

Magnetic tape drives are the most common backup medium, although other technologies are available. The tape drives record all the information entered that day in your office computer. To reduce tape wear and increase security, some practices use a separate tape for each day of the week.

Here are additional guidelines to make your backup process more reliable:

- Store long-term tapes (such as quarterly or annual practice records) off-site, in a secure, fire-resistant place.

- Check your backup system frequently. Remember that tapes, like hard drives, eventually fail. Replace your tapes regularly.

- Keep a signed "backup log" showing the dates when backups were done.

- Print periodic paper backups.

- Keep tapes away from heat and magnetic fields.

Electronic records are a viable alternative to traditional paper records in today's modern practice. By following sound risk management practices, you can enjoy the benefits a "paperless" system has to offer, while minimizing the risks of data loss or adulteration.

## Are Dentists Ready to Go Paperless?

Despite the improvements in electronic record systems, many dentists appear reluctant to make the leap. During our risk management seminars, we often ask attendees to raise their hand if they are keeping clinical patient notes in electronic form, rather than on paper. The responses have ranged from a few individuals to just over a dozen. So while we know that the vast majority of dentists have computers in their offices, and that many are now using features such as appointment scheduling in addition to billing functions, the dental profession as a whole has not yet embraced the record keeping facet of computerized practice management systems.

*This publication is for educational purposes only. It is not legal or dental advice. CNA makes no representations as to its correctness or completeness and accepts no liability for any injury or damage that may arise from its use. Specific legal or dental questions should be referred to a competent attorney or dental professional. This material may address and discuss matters for which your policy does not provide coverage, and the material does not create or imply the existence of coverage. Please consult your insurance policy for the specific terms and conditions of coverage.*