

HIPAA

the Good the Bad and the Ugly

The Health Insurance Portability and Accountability Act (HIPAA) may have its frustrating, bureaucratic sides, but its emphasis on timesaving electronic records and technology is a plus.

By Dr. Larry Emmott



DR. LARRY EMMOTT

American dentists face a daunting set of new federal regulations with the Health Insurance Portability and Accountability Act (HIPAA)—regulations that are the direct result of high-tech electronic systems.

There are many excellent sources of HIPAA information to help you deal with its regulations. These include the American Dental Association, which

runs HIPAA seminars and provides compliance kits, and the Office for Civil Rights (OCR), a division of the U.S. Department of Health and Human Services (HHS), which has detailed information about HIPAA

on its Web site. For a list of these and other sources, see the “HIPAA: online resources” sidebar on page 60.

This article, though, isn’t another checklist of regulations and deadlines. Rather, it’s a discussion of HIPAA’s purpose and the role technology plays in its implementation. For if you understand the why of the regulations, compliance makes more sense and becomes easier.

Like the classic Clint Eastwood western, HIPAA is good and bad and ugly. Signed into law in 1996, HIPAA is designed primarily to protect consumers from the capricious loss or denial of health insurance. For example, this could happen when an employer uses healthcare data to deny a person employment or benefits.

So where does technology, dentistry, and privacy come into play with HIPAA? In an attempt to control costs and increase the portability of healthcare plans, “the law requires all health plans, health clearinghouses, and any dentist who transmits health information in an electronic transaction, to use a standard format,” according to the ADA’s Web site.¹

So what’s good, bad, and ugly about HIPAA and using electronic formats? The good part is that electronic-data gathering saves time and money. The bad part is that electronic data can be used inappropriately. The ugly part is being stressed out about what HIPAA does and doesn’t require. Here are some facts about HIPAA and its electronic recordkeeping regulations that may ease the pain of regulation and documentation.

THE GOOD

Timesaving electronic records

Once all healthcare information is stored in a standard electronic or digital format, all kinds of wonderful things can be done with it. The data can be stored, transmitted, and enhanced electronically. That is the essence of the digital revolution.

It means patients will have a clear and complete health history without having to fill out endless forms every time they walk into a healthcare facil-

Good: It will improve the overall healthcare system and reduce costs through the use of electronic records.

Bad: Health data collected electronically could be used inappropriately.

Ugly: There is a lot of misinformation around. Don’t get caught up in it all.

ity. It means patient data can flow instantly and seamlessly between facilities. Electronic data will decrease costs and improve care.

What will be included in these electronic records? Here’s one scenario.

A typical medical record. A patient’s record can include the following information:

1. *Personal census information.* This includes name, address, and phone number.
2. *Financial information.* This mostly relates to health insurance.
3. *Clinical information.* This includes a health history, clinical findings, test results, x-rays, diagnosis, treatment, prescriptions, progress notes, and more. (Incidentally, the types of information described in 1. and 2. above are not regulated by HIPAA.)

If all of this information is on paper, then storing, copying, and transferring it can be slow and expensive. If it is digital, it can be stored, copied, and transmitted much more effectively.

A typical patient scenario. Before we look at the advantages of a digital system, let’s look at the following scenario for a patient traveling through a typical healthcare process:

- The patient starts with the general physician.
- Then, the patient is referred to a specialist for evaluation.
- From there, the patient goes to a clinic or to a lab for tests and diagnostics, such as x-rays, CAT scans, and MRIs.
- Then, the patient may be transferred to another office to complete the diagnosis.

Continued on page 56

Reigning in HIPAA

Here’s Dr. Emmott’s advice on how to deal with HIPAA’s regulations and bureaucrats.

- Designate a privacy officer
- Provide training
- Create a privacy statement
- Have all patients sign an acknowledgment form, and most importantly,
- Document all the measures you take.

Note: Who has to comply with the HIPAA privacy rule? “Any dentist who transmits protected health information electronically using HIPAA standard transactions or has someone do it on his or her behalf, such as a clearing house or vendor is a covered entity and must comply” according to the ADA.⁵

Continued from page 54

- Now, the patient is off to a hospital for surgery from yet another physician.
- Finally, after the patient leaves the hospital, the patient is given more prescriptions to take to a pharmacist and is sent to a different facility for physical therapy.

All together, the patient has seen at least nine healthcare professionals (two doctors, two technicians, a surgeon, several nurses, anesthesiologists, pharmacists, therapists) and been to six different facilities.

At each step, the patient is required to provide personal and insurance information and fill out a health history.

At each facility, staff members need to collect data about the patient, store it in a chart, and then transmit it to the next facility, to the patient, and to the patient's third-party payors.

By the way, the patient also received great care and recovered completely.

The value of a digital record. Compare the process of gathering the above patient data at each step and each facility, and on paper, to gathering patient data via a completely digital system.

With a digital system, the patient would provide the personal and financial information one time, and then the data would travel seamlessly, electronically, and instantly to the next five facilities that need it.

All the clinical data also would flow seamlessly from general physician to specialist to hospital to physical therapist.

And, finally, the insurance claims would be generated and sent instantly along with all relevant clinical data.


The patient still receives great care and recovers completely. However, in this scenario, it all happens faster, costs are lower, and the patient is hassled less.

Standardizing digital records. HIPAA has what are called "transaction and code set" standards that require health plans, billing services, and providers to use the same format for the electronic transmission of healthcare claims, according to the article, "Is Your Practice HIPAA compliant?" in *Day By Day*, a newsletter published daily during the Chicago Dental Society's midwinter meeting.²

In the article, the CDS suggests checking with your practice management software company for help in making your software HIPAA compliant. And, nationwide, software companies are working to help dentists with this task.

Help from software companies. Many software companies are incorporating the latest HIPAA information onto their Web sites. The on-

HIPAA forms on our Web site www.dentalproducts.net

To access examples of forms you may need to comply with the HIPAA privacy law, visit www.dentalproducts.net. From DPR'S home page, click on  and follow the "HIPAA" link. You will find seven forms in a printable format, including the "Privacy Policy Notice" and "Patient's Acknowledgment" forms shown below.*



*Forms are for informational purposes only. They are not for reproduction.

line information ranges from features on new software versions that help dental offices become compliant with HIPAA's electronic standards and codes, to answers to frequently asked questions about HIPAA, to forms doctors may want to have their business associates fill out, to deadlines for compliance with various electronic, privacy, and security standards.

Examples of such online sites include the following:

- a "HIPAA Update," section from Dentrix Dental Systems, a Henry Schein Company (www.dentrix.com),
- a "HIPAA Overview" section from PracticeWorks Inc. (www.practiceworks.com), and
- a "HIPAA Information," section (found under the Technical Support Services link) from Eaglesoft/Patterson Dental Supply Inc. (www.eaglesoft.net).

Many software companies also have a HIPAA expert available to answer questions from users. Although the deadline for compliance with electronic transactions was Oct. 16, 2002, dentists could extend that deadline to Oct. 16 of this year, but only if they filed for an extension.

THE BAD

Misuse of electronic records

Once all that personal health data is stored in a common electronic format, it can be retrieved, collated, and reviewed easily. That's good—if the health data is being used by the proper medical personnel. But, what if the gathered health data is available to others?

Scenarios. Here are some scenarios for the potential misuse of electronic health data. What if:

- Companies use the data to isolate certain individuals with specific illnesses, and then the companies attempt to sell them an unproven cure?
- Employers use the data to deny employment to certain groups?
- Insurance companies use the data to restrict benefits?
- A lender uses your health status to deny you a loan?
- Your neighbors see a list of drugs you are taking?
- Or worse yet, the public learns how much you weigh?

To prevent abuse of the system, the law

provides for privacy rules. It is those rules we are now seeing as the dreaded HIPAA privacy regulations, which went into effect on April 14. The regulations are very specific. They apply only to electronically transmitted information and only to protected health information (PHI).

In essence, the HIPAA privacy regula-

tion is common sense—is is not intended to restrict appropriate use of health information, and it is not aimed at a typical dental office. All dental-office personnel already should know that they never reveal patient health information unless the patient has agreed to this in advance. HIPAA is nothing more than what most dental of-

fices already do, with one ugly exception, as follows.

THE UGLY

HIPAA myths

Just as with OSHA, when dealing with government bureaucrats regarding

Continued on page 60


What's online




To quickly search for forms, facts, and products that have to do with the new HIPAA regulations, visit www.dentalproducts.net. On the home page, type in "HIPAA" in the search field at the top of the page. A "Search Results" page will include a link to "Management" articles about HIPAA and a New Product Search," which shows a list of HIPAA-related products.



Continued from page 57

HIPAA, it's not so much what you do, as what you document. For a look at some of the measures, including creating a privacy statement, that you can take to comply with HIPAA, see the sidebar, "Reigning in HIPAA" on page 54. And for a copy of some of the privacy forms you'll

need to comply with HIPAA requirements, see the sidebar, "HIPAA forms on our Web site: www.dentalproducts.net" on page 56.

As often happens with well-intentioned government intervention, though, there have been many unintended consequences of HIPAA. The most obvious is a mass of

hysterical misinformation. Unfortunately, entrepreneurs and telemarketers have spread much of the hysteria by using high-pressure sales tactics to scare dentists into buying HIPAA compliance products.

The misinformation problem is discussed in a Jan. 20 *ADA News* article, "HIPAA advice: Don't buy what you don't

need."³ The article warns dental office staff to beware of entrepreneurs who use high-pressure sales tactics to scare dentists into attending their HIPAA courses or who call dental offices to advertise consultants and products related to privacy rules under HIPAA. "Seek clarification from the ADA" if you are concerned about high-pressure HIPAA sales calls, the ADA suggests.

Myths. Another consequence of HIPAA is dentists' concerns about what they can and can't do under the law, such as the following scenarios:

- Dentists won't be able to use sign-in sheets or call out a patient's name in a reception room.
- It will be illegal to place a patient's chart in a plastic box outside a treatment room.
- You won't be allowed to leave a voice message on a patient's telephone, or mail or e-mail a card to a patient.
- You will need to monitor and get privacy agreements from the janitorial service as well as anyone else with access to your office.
- You won't be able to fax health information from your office to another dentist.
- Your office will be violating HIPAA rules if it gives a written Rx to anyone but the patient.
- All dental office rooms will need to be sound proof.
- Appointment reminders aren't allowed.
- Dental software companies are covered entities, and you will need a business associate agreement (BAA) from them. (Ac-

HIPAA: Online resources

Dr. Emmott's list of Internet sources for accurate HIPAA information include the following:

ADA Online

This site is very complete and includes access to the ADA compliance kit and seminars.
www.ada.org/prof/prac/issues/topics/hipaa/index.html

Office for Civil Rights (OCR), the official government site

OCR is the U.S. Department of Health and Human Services agency responsible for enforcing the HIPAA privacy rule.
www.hhs.gov/ocr/hipaa

HIPAA Advisory

This site is sponsored by Phoenix Health Systems.
www.hipaadvisory.com

Workgroup for Electronic Data Interchange (WEDI)

This site offers the "Small Practice Implementation" guide, a 56-page manual from WEDI.
www.wedi.org/snip/public/articles/2002_0510_1.2.pdf

According to HIPAA, a business associate is any person or organization that performs a function on behalf of a covered entity, such as dental office, but is not part of that entity.)

All of the statements above (except possibly the last one) have one thing in common: **they are false**, according to the HHS/OCR Web page on HIPAA (www.hhs.gov/ocr/hipaa).⁴

Note: A possible exception is the last scenario—needing to have a BAA with your software vendor. You would need to have your vendor sign a BAA if the vendor would be handling your protected health information (PHI) in any form.

This might happen, for instance, when your software company is doing a database repair for you or looking at a screen shot to correct some aspect of a software program. Such cases are rare, but if for any reason, a business associate handles your PHI, an agreement covering both parties under HIPAA is needed. Check with your software company, which may provide you with a BAA form to cover such cases.

A common sense approach. When faced with wild HIPAA privacy questions, though, don't panic; use common sense. Ask yourself:

Does the issue concern protected health information?

Answer: Names and addresses are not protected information.

Does the issue involve electronic transmission of information?

Answer: Remember—talking with a patient in the office is not electronic.

What is the real issue?

Answer: It's not to prevent you from providing care; it is to prevent the improper use of health information.

HIPAA is good: It will improve the overall healthcare system and reduce costs. It is bad: Health data collected electronically could be used inappropriately. It is ugly: There is a lot of misinformation around. Don't get caught up in it all.

Nevertheless, you will need to comply with HIPAA now and in the future—and I still believe, the future is coming and it will be amazing! **DPR**

site at www.drarryemmott.com, or he may be reached at 602-279-1641.

References

1. American Dental Association. Health insurance portability and accountability act (HIPAA). Available at: www.ada.org/prof/prac/issues/topics/hipaa. Accessed April 1, 2003.
2. Parry V. Is your practice HIPAA-compliant? Day by Day, March 1, 2003. Chicago Dental Society. (Note: Day by Day is a CDS publication that appeared daily during the 138th Midwinter Meeting, Feb. 27-March 2, 2003.)
3. Furlong A. HIPAA advice: don't buy what you don't need. ADA News 2003;34(2):1,15.
4. U.S. Department of Health & Human Services. Office of Civil Rights. Questions and answers about HIPAA. Available at www.hhs.gov/ocr/hipaa. Accessed April 2, 2003. (Note: to access the Q&A list on the HIPAA page, click on "What's New," scroll

- down to "3/13/03 New FAQs providing answers ...," and then look for an "FAQs" link in the text.
5. Furlong A. HIPAA privacy deadline is April 14. ADA News 2003; 34(6):14.

Dr. Larry Emmott, a recognized authority on dental technology in America, is a practicing general dentist in Phoenix. He also is an award-winning professional speaker, a featured instructor at the Las Vegas Institute, and a member of the American Academy of Dental Practice Administration. He has written hundreds of articles on dentistry, computer use, and management. Since 1995, he also has written a monthly electronic newsletter, "Emmott on Technology," on using dental technology effectively. Dr. Emmott offers hands-on technology seminars to selected dentists in his Phoenix office (the next one is Oct. 3-4). At these seminars you will receive personalized advice on setting up your office to maximize your high-tech future. Topics include digital radiology, cosmetic imaging, and treatment room design. To find out more, check Dr. Emmott's Web