HIPAA and Its Implications for Dental Hygiene

By Trudy Ring

Privacy—it's something we all value, even if there's nothing particularly sensitive in our personal information that could possibly be used against us. Just the same, we like to know that certain information will be disclosed only to the people to which we choose to disclose it. And patients of those working in health care services want to know that they can trust that their information will not be shared with anyone who does not have a legitimate need to know it.

As of April 14, 2003, the management of patients' information will be held to some new privacy standards. These standards, part of the Health Insurance Portability and Accountability Act (HIPAA) of 1996, will require some extra work on the part of dental offices, although opinions vary on just how difficult this work will be.

"They go much further than what patients had in the past, as far as rights," says Los Angeles-based attorney Scott A. Edelstein, Esq. "Certainly, implementing them is burdensome on practitioners—there's no doubt about it. But I have the feeling the burden is going to be short-term." Once health care providers have all their policies and systems in place for adhering to the standards, the work will be largely done, adds Edelstein, a partner in the firm of McDermott, Will, and Emery.

When Mary F.H. Baughman, RDH, MA, who practices in Sandusky, Ohio, was assigned to be HIPAA coordinator for one of the two offices she works in, she says that she was told, "It [will be] a massive job requiring many hours." Her experience, so far, has turned out somewhat different. "The many hours are just reading all the advice and information."

As of April 14, 2003, the management of patients' information will be held to some new privacy standards.

When Mary F.H. Baughman, RDH, MA, was assigned to be HIPAA coordinator for one of the two offices she works in, she says that she was told, "It [will be] a massive job requiring many hours."

On the other hand, Judith Corbin, RDH, BSDH, FADPD, says a dentist she knows told her he intended to retire before April 14 so he would not have to deal with the HIPAA mandates. Corbin is in charge of making sure the office where she practices, in Thomasville, Georgia, is in compliance with HIPAA. She says, "It takes a lot of time to do this, and I can't see that it is going to take any less time."

To Kitty Harkleroad, RDH, BS, compliance officer for the dental hygiene department at the University of Tennessee, Memphis, "The HIPAA regulations are necessary and appropriate." But, she says, "As with any government regulations, there is always lots of paperwork involved. I don't think these new privacy and security regulations will be a big burden to private practices, but it will require some planning, policy writing, and training of employees. The main thing that will have to change is attitudes and habits." How much time is involved in compliance will depend on the size of the practice, Harkleroad adds.

Just What Is Required by HIPAA?

The overall purpose of the act, signed into law by then U.S. President Bill Clinton on August 21, 1996, is to make it easier and more affordable for Americans to obtain health insurance. HIPAA prohibits group health plans from denying or charging extra for coverage because of a person's past or present poor health. It also limits the degree to which preexisting conditions can be excluded from coverage, guarantees certain small employers (and certain individuals who have lost job-related health benefits) the right to buy health insurance, and guarantees that most employers and individuals can renew their insurance regardless of the health of anyone included in the policy.

The law has a provision called Administrative Simplification, which seeks to make it easier to carry out such tasks as submitting claims, thereby lowering the associated costs. HIPAA aims to make possible the standardized electronic transmission of claims and other information. It does not require any health care provider to submit electronically, but it does set rules that providers must follow when they send claims or any other information electronically—and here is where privacy comes in.

The Price of Privacy

Recognizing that circulating health information electronically would raise concerns about privacy, the Administrative Simplification provision called on Congress to develop regulations governing privacy within three years of HIPAA's enactment—or, if Congress did not do so (and it did not), for the U.S. Department of Health and Human Services (HHS) to perform this task. HHS released what was to have been the final privacy rule in December 2000, but after President George W. Bush took office in 2001, his HHS secretary, Tommy G. Thompson, requested additional public comment on the rule. After receiving more than 11,000 comments, HHS put together a new proposed rule in March 2002 and issued a final one in August 2002. Most of the entities subject to the rule have until April 14 of this year to comply. These entities include insurance plans, health care clearinghouses, and health care providers who transmit patient health or demographic information electronically.

The privacy rule generally allows providers and other entities to disclose patient information only to the degree necessary to accomplish a given purpose—say, to provide care or arrange for payment from an insurer. It also allows patients to find out what pieces of their information have been disclosed and how they might be used, as well as to obtain a copy of their medical records and to request that errors be corrected.

Health care providers must provide patients with written information about their privacy rights; adopt privacy procedures for their offices, such as making sure patient records are kept in a secure place; make records inaccessible to those who do not have a legitimate need to view them; make sure all employees receive training about privacy policies; and designate a person to be responsible for seeing that everyone adheres to these policies. Also, what HIPAA calls "business associates"—companies that do business with entities that answer to the act and have access to patient information, such as a dental laboratory or a firm that handles billing—must sign an agreement stating how patient information will be protected from unlawful disclosure.

"The privacy notice is probably the most troublesome thing at this point," says Rebecca Reynolds, BS, MS, MHA, an assistant professor in the health information management program at the University of Tennessee, Memphis. In drafting the notice, providers must make sure it's appropriate to patients' reading levels and therefore understandable to them, she notes.

If a state has a privacy law that is stronger than HIPAA's privacy rule, it will supersede HIPAA, Edelstein says, adding that California, Florida, and Texas are among the states that already had stringent laws in place regarding patient privacy, he says.

There are two other aspects of the Administrative Simplification provision, security standards and the use of a standard set of codes in transmitting health care information electronically. Providers were required to comply with this by October 16 of last year if they did not file a request for a one-year extension, which many have done. The extension had to include a plan showing how the provider would achieve compliance before October 16, 2003.

Is Electronic Data Transmission Better?

HHS's rationale for standardizing codes is that this will make electronic data transmission more efficient and result in cost savings for health care providers and other covered entities. In 2000, upon releasing the final version of the code sets regulation, HHS estimated that there were about 400 different formats for health care claims in use in the United States; they noted that the lack of standardization made it hard to develop and maintain software to handle claims transactions.

HHS requires that the codes come from an organization accredited by the American National Standards Institute (ANSI). The standard code set that HHS has designated for oral health care services is the American Dental Association's (ADA) Code on Dental Procedures and Nomenclature, published as *Current Dental Terminology*. Under the law, health care providers, insurers, and clearinghouses

Judith Corbin, RDH, BSDH, FADPD, says one dentist she knows told her he intended to retire before April 14 so he would not have to deal with the HIPAA mandates. Corbin is in charge of making sure the office where she practices, in Thomasville, Georgia, is in compliance with HIPAA. She says, "It takes a lot of time to do this, and I can't see that it is going to take any less time."

The overall purpose of the act, signed into law by then U.S. President Bill Clinton on August 21, 1996, is to make it easier and more affordable for Americans to obtain health insurance.

do not have to use the standard code sets for paper transactions, but certainly may do so if they choose to.

Offices that do not file electronic insurance claims are not be affected by this section of the law. However, Harkleroad notes that "offices that still file paper claims may be interested to know that by October of this year, Medicaid will accept only electronic claims. It only makes sense that major insurance companies will follow suit, and additional fees will be charged for accepting paper claims." Offices that do not file claims electronically still must comply with the privacy rule and with the other aspects of Administrative Simplification that address security standards, she says. "Unless an office uses no computers, no fax machines, and no telephones, they do transmit electronic data and therefore are not exempt from HIPAA."

Security Standards

Final security standards were published in the *Federal Register* on February 20, 2003. They have an effective date of April 21 of this year with most covered entities given until April 21, 2005 to comply (small health plans were given an additional year). The rule laying out the final standards notes, "Security and privacy are inextricably linked. The protection of the privacy of information depends in large part on the existence of security measures to protect that information." However, it goes on to list several differences between the privacy rule and the security rule. The security standards lay out "administrative, physical, and technical safeguards," while the privacy rule governs the use and disclosure of patient health information and patients' right to control it.

The security rule states that health care offices must use both physical and technical safeguards to control access to patient information that is in electronic form. The issue of whether computer workstations are behind closed doors, for instance, falls under physical security; the matter of using protections such as passwords and encryption to control who can see a computerized record falls under technical safeguards.

Health care entities will have some flexibility in complying with the security rule. They are required to limit physical access to electronic information systems while making properly authorized access possible, but they can determine for themselves how to do so. They are also required to assign unique names or numbers to identify all people who use the electronic systems, but encrypting data or using an automatic logoff feature to end computer sessions are optional. The security rule notes that because the entities responsible to HIPAA vary so much in size and type, it would be impossible to dictate a specific solution for all of them, and the government decided not to prescribe specific technological measures because technology is constantly evolving.

There will be significant similarities in complying with the security and privacy rules, says Beth Kost, BS, RHIA, vice president of Precyse Solutions, a company that provides health information management services to health care providers. "Security is looking at systems, primarily," she says. "But there are many places where [privacy policies and security policies] overlap." Health care offices most likely can write one policy for privacy, then just change a few components and have a policy for security, she says.

However, right now implementing the privacy rule is a priority for health care providers. "The pri-

vacy rule basically governs the use and sharing of health care information," Edelstein says.

The rule requires health care offices to post in a conspicuous area a notice explaining how patient information will be used and kept from unauthorized or inappropriate use. It also requires that patients be provided this notice when they come in for treatment, and that health care offices make a good-faith effort to obtain patients' written acknowledgment that they have received the information. This is less restrictive than originally planned. Before the rule was modified by HHS last August, it called for health care providers to obtain patients' written consent before using individually identifiable patient information for treatment, payment, or administrative purposes. In issuing the modified rule, HHS Secretary Thompson said the original one could have required a patient to sign forms at a pharmacy or a medical specialist's office before the pharmacist or specialist could review the patient's protected health information.

Patients will have to give written consent if a health care provider is going to use their information for marketing purposes, with exceptions for face-to-face communications such as referring the patient to other services and promotional offers involving gifts of nominal value. It is not considered marketing when a health care worker tells the patient what other services the worker's own practice offers.

Kost says that when HHS initially proposed modifications to the privacy rule, she was concerned that patient privacy was being threatened, but she is satisfied that the final rule lets patients know their privacy rights in no uncertain terms.

Also, the August modifications by HHS let health care workers know it would not violate the privacy rule if they called out patients' names in the office or had patients sign in upon arriving for their appointments. In the course of a conversation to keep incidental disclosure of patient information from being overheard—say for instance during a chairside conversation between patient and dental hygienist or a consultation between the dental hygienist and dentist—the rule requires health care providers to take reasonable precautions. For example, if a private room is available, the conversation should be conducted there. But, at the same time, there is nothing that states dental offices will have to remodel in order to put in private rooms or hospitals have to erect walls in-between beds.

Compliance May Be Closer than You Think

In the past, willingness to disclose patient health information may have been greater in the oral health care field than in other health disciplines, according to Edelstein. He says this is largely because information about a person's oral health is often not perceived as being as sensitive as information about other health problems or procedures. Because of this, Edelstein says, "I think dental practices, to some extent, are going to have a bigger adjustment [in complying with HIPAA privacy standards]."

Oral health practices have traditionally not been as heavily regulated as other health care providers, Reynolds adds, so some of the issues involved in compliance will be new to them. "Some of this stuff you should have been doing already," she says. "Some people were and some people weren't."

However, many oral health offices have

HIPAA does not require any health care provider to submit electronically, but it does set rules that providers must follow when they send claims or any other information electronically—and here is where privacy comes in.

The privacy rule generally allows providers and other entities to disclose patient information only to the degree necessary to accomplish a given purpose—say, to provide care or arrange for payment from an insurer.

long been adhering to the type of privacy practices enshrined in the law, or even going beyond them. "We have never had patients sign in," Corbin says. "We have had them complete registration forms in private and have had a permission policy for photos, videos, and slides in place for some time. Reminders are sent as letters, not cards." She adds that her office has converted one room to a chart room, to which only she has the key, and is no longer posting schedules of appointments on the wall.

"Most of the regulations regarding privacy are already being observed in private dental practices, since the dental community has always respected patient privacy," Harkleroad says. "The difference now will be that policies will have to be composed and documented."

Kost adds, "These are really good practices about patient confidentiality and patient protection, and things we should have been doing all along. Many times, providers have policies and procedures that are in compliance and they just don't realize it."

Still, Corbin sees HIPAA compliance as taking time from patient care and as something likely to be more onerous in practices larger than her one-dentist, two-dental-hygienist office. "I can keep my finger on the pulse of this office really well," she says. "The privacy rule probably would not be necessary if all health care practitioners had conducted their business ethically all along."

"Average dental practices are not the problem, and not why the law was originated," Harkleroad says. "Insurance clearinghouses, hospitals, and large clinics are the ones targeted by this law, since lots of private information flows through them. But the law has to apply to all health care providers to be fair and consistent. Identity theft and selling of patient lists to private businesses are everyday occurrences today, and the government stepped in to try and reduce these problems for health care consumers.

"Dentists who choose to not comply can be hit with heavy fines and possibly jail time," Harkleroad says. "Patients will begin hearing about HIPAA and their rights, and see changes at their doctor offices and hospitals. They will want to know why their dental office is not doing the same things, if it is not."

Baughman says she has not found compliance to be a particularly time-consuming effort, except for her aforementioned hours of reading and study. "As far as what we actually do, we contacted our software vendor for paperwork and information, we bought a shredder and, item by item, we are quietly implementing privacy procedures we'd planned and had been implementing anyway," she says.

One new development oral health practices may see down the road is an increase in requests from patients for their records, Reynolds says. "Our dental office does not get nearly as many requests for records as do our medical offices," she says. "I don't know if that will change." If it does, Reynolds says it could be a major change.

There are many different types of software available to assist in compliance with the HIPAA privacy rule and code sets; some of these are extensive tool kits that include such components as online training in HIPAA adherence or downloadable patient privacy forms in both English and Spanish. HIPAA will not necessarily result in all health care practices having to buy new software, but Edelstein says, "Most likely, at the very least, it will require practitioners to look at their existing systems." Some oral health practices, particularly small ones, may not have adequate software in place, he says. In shopping for software, he adds, "It's going to be up to the individual practitioners to decide if they want to rely on the presentations of the vendors or hire a consultant."

Kost notes that there are some software packages that assist with overall regulatory compliance that can integrate features needed to adhere to HIPAA. "There are some companies that have done a good job of pulling that all together," she says. She recommends that health care providers

HIPAA Privacy Checklist

The HIPAA privacy compliance date is April 14, 2003. It's time to assess your readiness. Get started with the ADA HIPAA Privacy Checklist, part of the ADA Privacy Kit. The complete kit, which will be available by August, tells dentists more specifically what they need to know to comply with the HIPAA Privacy Rule, as presently proposed. **To make your dental office compliant by April 14, 2003:**

Task	Planned Completion Date	Completed by 4/14/03
Develop a compliance timeline, using this checklist as a starting point.		☐
Learn what HIPAA requires and do a gap analysis to assess where your current practices may be lacking.		☐
Develop privacy policies, procedures, and documentation practices.		☐
Develop necessary forms to implement your policies and practices (for example, Acknowledgement of Receipt of Notice of Privacy Practices).		☐ ☐
Develop a Notice of privacy practices to post and give to patients, and a method to document your good faith attempt to secure patients' acknowledgment of receipt of the Notice.		☐
Designate a privacy officer and a contact person to receive complaints.		☐
Train employees in privacy. Document all training efforts.		☐
Develop an employee discipline process for privacy violations.		☐
Evaluate which of your relationships requires a Business Associate (BA)		☐
Agreement and enter into the required written contracts, using BA agreement language satisfying HIPAA's specific requirements. (Compliance date is April 14, 2004 for amending existing written BA agreements, but those that are renewed or modified before then must be amended at the time of that renewal or modification.) Your dental office should have appropriate administrative (for example, policies, procedures and staff training), technical (for example, secure software and passwords), and physical (for example, doors and locks) safeguards in place to make sure health information is private and secure.		☐ ☐

To remain compliant during the operation of your practice:		Completed by 4/14/03
Implement procedures to verify identity and authority to access, receive or use what is protected health information (PHI) under HIPAA. Keep in mind that PHI includes oral communications (for example, verbal communications among staff members, patients, and/or other providers).		☐
Secure the right to use or disclose PHI. For purposes of treatment, payment, and healthcare operations (TPO), your good faith attempt to secure an Acknowledgement of receipt of your Notice of Privacy Practices will suffice. Otherwise, secure a written authorization as required by HIPAA.		☐
Plan to use PHI information by applying the minimum necessary standard, which will often require that you make reasonable efforts to use or disclose only the information that is needed to accomplish the intended purpose.		☐
Know what patients' federal rights are established by HIPAA, and develop processes to ensure you will honor those rights (for example, the rights to access and copy protected healthcare information; the right to amend a patient record; the right to an accounting of disclosures; and the right to confidential communication and so on).		☐
Implement complaint systems.		☐
Know the HIPAA marketing rules and follow them.		
Limit the consequences if there is a breach of confidentiality by you and/or your business associate.		☐
Develop and implement a HIPAA privacy self-audit program to make sure your compliance efforts are working.		☐
Document, document, document!		☐

***The Checklist does not assure compliance with HIPAA or constitute professional advice. Dentists must consult with their professional advisors for such advice.**

The American Dental Association's privacy kit is available by calling 800/947-4746 and online at www.adacatalog.org.

Dental hygienists say that implementing HIPAA's privacy provision calls for contributions available only from the human element—professional ethics and common sense.

"look at pulling in those packages that do as much as possible."

Reynolds says that until software has been tested in actual transactions, it's impossible to know whether it's fully compliant. "Talk to your colleagues," she advises. "You don't want to be stuck with a system that's not compliant."

Professional associations also can help health care providers understand and implement HIPAA's rules. Reynolds is preparing a continuing education course on HIPAA for the American Dental Hygienists' Association (ADHA) that will be published in ADHA's *Journal of Dental Hygiene*. ADHA also has information on compliance on its Web site. ADA has offered privacy seminars at meetings of state and local dental societies and has put together a compliance kit that includes a CD-ROM of customizable forms. Corbin notes that she attended an ADA seminar through the Georgia Dental Association. And Reynolds adds that the American Health Information Management Association (AHIMA) and the American Health Lawyers Association (AHLA) are good sources of HIPAA information.

HHS itself is offering assistance as well. Its Office for Civil Rights (OCR) is enforcing the privacy rule. OCR's Web site has downloadable documents on significant aspects of the rule, plus a question-and-answer feature to help health care practitioners determine if they constitute a covered entity under the law. OCR also conducted conferences on privacy in Atlanta, Chicago, New York City, and San Diego in early 2003. Another division of HHS, the Centers for Medicare and Medicaid (CMS), is enforcing the code set and security standards of HIPAA. Extensive information is available on CMS's Web site.

Dental hygienists say that implementing HIPAA's privacy provision calls for contributions available only from the human element—professional ethics and common sense. "Everybody needs to adhere to strong standards of ethics," Corbin says.

Harkleroad reminds: "As patients, we all want our privacy protected, and we must do the same for our patients."

And Baughman notes, "I also see paranoia possibilities; some people go overboard with their perceived responsibilities. We could turn the office into a police state or we could be lax. My goal is to be reasonable and considerate. That's what we should be doing anyway."