THE DENTAL CLINICS OF NORTH AMERICA

Dent Clin N Am 46 (2002) 553–563

The Health Insurance Portability and Accountability Act: implications for the dental profession

Rosemary Walker, DDS, MBA, MS

University of Illinois at Chicago, College of Applied Health Sciences, School of Biomedical and Health Information Sciences, 1919 West Taylor (M/C 530), Chicago, IL 60612, USA

In 1996, President Clinton signed the Health Insurance Portability and Accountability Act (HIPAA), a law that would transform the management of health care. HIPAA was written to address many health care issues, such as the portability of health insurance coverage, promotion of medical savings accounts, control of waste, fraud, and abuse in health insurance and health care delivery, and improved access to long-term care services and coverage. Included with these issues is a section entitled "administrative simplification." The intent of this section is to "improve… the efficiency and effectiveness of the healthcare system by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information" [1]. The privacy of the patient also would be protected.

The Department of Health and Human Services (HHS), then under the direction of Secretary Donna Shalala, was selected to coordinate the massive task of implementing administrative simplification. The result was a series of proposed rules, posted beginning in 1998, that provided enforceable requirements with specified deadlines. These rules were directed at all health care entities that send standard electronic transactions carrying individually identifiable patient health care information. These entities included, but were not limited to, hospitals, insurance companies, dental and medical schools, dental and medical practitioners, prison health systems, government health systems, laboratories, and pharmacies. Noncompliance was not an option.

The proposed rules initially covered the following areas: (1) electronic transactions and code sets, (2) privacy standards, (3) security and electronic

E-mail address: rwalke7@uic.edu (R. Walker).

PII: S0011-8532(02)00009-5

signature standards, (4) national standard health care provider identifiers, and (5) national standard employer identifiers. Eventually, proposed rules will be posted for (1) health plan identifiers, (2) individual identifiers, (3) claims attachment transactions, and (4) first report of injury transactions.

HHS provided a period of time for the industry to respond to the proposed rules. After considering the many responses, it released the first of the final rules, electronic transactions, on August 17, 2000 (Table 1). When the first rule on electronic transactions appeared with a deadline of October

Table 1
HIPAA summary table

Rule	Final/ proposed	Date published	Compliance date	Implications
Electronic transactions	Final rule	August 17, 2000	October 16, 2002 with extension, October 16, 2003	Data format and content of specified electronic transactions must follow HIPAA standards
Privacy	Final rule	December 28,2000	April 14, 2003	Documented practices and procedures that protect PHI must be established; these include training the staff and developing consent forms, notice of privacy practices, business associate contracts
Security	Proposed rule	August 12, 1998	Unknown	Current security practices need to be evaluated; documented security policies and procedures must adhere to HIPAA requirements; these include administrative initiatives, physical safeguards, and technical modifications
National provider identifier	Proposed rule	May 7, 1998	Unknown	HIPAA covered entities must use this number in HIPAA transactions; Method of issuing identifiers is still unknown
National employer identifier	Final rule	May 31, 2002	July 30, 2004	The employer identification number (EIN) is not required in standard transactions conducted by dentists

2002, the health care industry slowly awakened to the ramifications of HIPAA. The final privacy rule, posted in December 2000, delivered the coup de grace that left the health care industry reeling. The resultant outcry by health care organizations against HIPAA was fueled by the realization that implementation would require massive technical and administrative changes that may not be met within the time constraints and could be cost prohibitive. The required efforts to achieve implementation successfully would far surpass those required to address the Y2K problem.

Interestingly, the health care industry had attempted for years to standardize the collection and use of patient information, desiring the same goals as HIPAAs simplification provisions. The government stepped in only after the industry's attempts had failed.

After the posting of the privacy final rule, certain health care organizations spearheaded attempts to postpone the deadlines, whereas others sought modifications of the rules, an action allowable by law. In April 2001, the Bush administration put the privacy rule into effect, which required an implementation date of April 2003.

HHS plans to release modifications and guidelines for the privacy and transaction rules to ensure that the rule can be implemented realistically. The first guidance to the privacy rule was released July 6, 2001 to elucidate discrepancies in the final rule. Modifications were proposed March 27, 2002. At the time of this writing, the only other final rule published is the national employer identifier that was released May 31, 2002.

Health Insurance Portability and Accountability Act and dentistry

HIPAA impacts all health plans, health care clearinghouses, and health care providers who transmit health information via standard electronic transactions. They are known collectively as "covered entities." A health plan includes government (military health system, veterans health administration, Indian health service, Medicare/Medicaid) and private sector health plans. A clearinghouse converts a dentist's nonstandard transactions to standard transactions and back again, which ensures that the appropriate parties, usually the dentist and insurance companies, receive the proper transactions.

All health plans and clearinghouses are obligated to adhere to HIPAA requirements, but not all dentists fall under the HIPAA umbrella. Practitioners who work in paper environments or simply store data in computers are not required to be HIPAA compliant. Dentists are not required to purchase computers in response to this law. If a dentist uses a clearinghouse to transmit his or her transactions, however, then the dentist is responsible for HIPAA compliance. Associates and hygienists are not covered entities under HIPAA when they are considered members of the workforce.

As a result of HIPAA implementation, dentists should realize the benefits of increased administrative efficiency and effectiveness with ensuing lowered

operating costs. Patients should feel that their privacy has been protected by proper security methods.

HIPAA recognizes that the size of an organization affects the degree to which the rules necessitate adherence. A small dental practice does not have the same scope of HIPAA obligations as a dental school or an insurance company. Because of a small working environment with relatively simple computer needs and a lack of volume of protected health information (PHI), a practice's policies and procedures are limited.

Regardless of the size, unless an entity is defined as a small health plan, an organization must comply within 2 years and 2 months of the posting of a final rule. The privacy rule was a timing exception caused by an error in procedure. Currently, the Office of Civil Rights (OCR) is responsible for implementing and enforcing the privacy rule, and HHS may regulate the remainder of the rules. An enforcement final rule will be published to provide further information. Penalties have been established for noncompliance.

Standards for electronic transactions

An average of 26 cents of each health care dollar is spent on such tasks as checking patient eligibility, processing claims, determining claim status, and notifying a provider about the payment of a claim [2]. It is not surprising that most dental practices spend a great deal of time each day making insurance-related phone calls and dealing with myriad claim forms.

Through the standardization of electronic transactions that use only one code, dental staff personnel can submit for a dentist to any health care plan using a single format for each of the following transaction types:

1. Health care claims and equivalent encounter information
2. Enrollment and disenrollment in a health care plan
3. Eligibility for a health care plan
4. Health care payment and remittance advice
5. Health care plan premium payments
6. Health care claim status
7. Referral certification and authorization
8. Coordination of benefits

Health care plans must accept an electronically submitted standard claim and cannot delay its payment. Plans also cannot require a dentist to change or add to the claim form. Should a health care plan use a clearinghouse or operate as one, the dentist must not pay more to use the clearinghouse than if he or she dealt directly with the plan [3].

The dental code recognized by HIPAA is the Code on Dental Procedures and Nomenclature (CDT-3), which is available from the American Dental Association (ADA). Dentists, in some instances, may also rely upon CPT-4 (Current Procedural Terminology, 4th edition), ICD-9-CM (International Classification of Diseases, 9th revision, Clinical Modification), and HCPCS

(Health Care Financing Administration Common Procedure Coding System). Codes will be updated as needed. The law does not require that codes should be available at no charge but that they should be distributed in an efficient, low-cost manner.

At the time of this writing, there was no claims attachment standard. Dentists must continue to mail charting and radiographs to insurance companies or send them using a nonstandard electronic format.

The current standards are based on electronic data interchange, which includes the use of the Internet. Some dentists also may use direct data entry as a means of transmitting data to an insurance company. In this instance, a dental staff member enters data directly into the plan's computer system via dumb terminals or Web browsers. Direct data entry is an acceptable mode of transmission as long as the data content follows the X12N requirements. Data content simply means the CDT-3 codes and data elements (eg, the procedure date). The same data content requirement pertains to fax back, hypertext markup language (HTML), and telephone voice response. Use of extensible markup language (XML), which is quickly becoming a standard for e-commerce, is not recognized by HIPAA. New standards, however, are considered for acceptance if they have become industry standards.

Government agencies were not used in the development of these standards. All transactions are from the private sector's Accredited Standards Committee X12N, except for the standards for retail pharmacy transactions. The ADA played an active role in the development of transaction standards and provided the CDT-3 codes. The ADAs Dental Content Committee provides input by making recommendations to the Secretary when there are suggested changes to the standards. Each year, HIPAA permits the adoption of new standards or the modification of old versions. A proposed rule was published May 31, 2002 providing limited technical modifications to several of the standards, specifically the implementation standards found in the final rule.

The disadvantage of the electronic transaction rule is the cost to a dentist who currently sends electronic transactions who must then pay for the conversion costs of his or her patient management system. A practitioner previously using paper claims and wishing to benefit from the standard must purchase computer hardware and software or contract with a clearinghouse to handle the transactions.

The benefits from using the rule should outweigh the cost of software upgrades. The dentist should recognize a reduction in administrative costs, accurate and timely processing of claims, assurance of security and confidentiality of individual data, and a marketing advantage [4].

While a dentist must comply with the electronic transactions rule by October 16, 2002, the deadline may be postponed until October 16, 2003 if adentist submits a compliance extension plan on or before October 15, 2002. See http://www.aha.org/hipaa/resources/Content/HR3323.pdf for more information.

Privacy

Privacy can be defined as a person's right to permit access to his or her personal information, including health care information. HIPAAs privacy rule marks the first time the federal government has stepped in to protect the privacy of health care information. This rule only applies to the covered entities: health care plans, health care clearinghouses, and providers who conduct standard electronic transactions. It covers their entire written, oral, and electronic PHI.

Under HIPAA, patients have certain rights. A dentist is required to provide a patient with a written explanation of how the office may use and disclose his or her health information. Patients must have the ability to access their records, request amendments, and receive copies of their records upon request. In the event of privacy violations, patients can file a formal complaint with the dentist or OCR.

March 27, 2002 HHS proposed certain changes to the final privacy rule to "maintain strong protections for individually identifiable health information while clarifying misinterpretations, addressing the unintended negative effects of the Privacy Rule on health care quality or access to health care, and relieving unintended administrative burden created by the Privacy Rule" [5]. Of interest to dentists are the changes in regards to patient consent, notice of privacy practices, oral communications, and parameters for minimum necessary disclosure.

Attaining patient consent will be optional for the use and disclosure of the PHI for TPO (treatment, payment, and health care operations). HHS proposes, however, that a dentist may obtain consent if he or she chooses, notice requirements be strengthened to "preserve the opportunity for individuals to discuss privacy practices and concerns…" and the consent process be flexible for those who choose to obtain consent. Uses or disclosures of PHI for TPO would need to be consistent with the notice of privacy practices [5].

An authorization is a more customized document than a consent form that gives a dentist "permission to use specified PHI for specified purposes, which are generally other than TPO, or to disclose PHI to a third party specified by the individual" [6]. A history of nonroutine disclosures must be available for the patient upon request.

The privacy rule specifies the content of the notice of privacy practices. It also states that a dentist in a direct treatment relationship with a patient must provide the notice by the first service delivery date. He or she must also make a good faith effort to procure the patient's written acknowledgment of receipt of the notice at the first service delivery, except in emergency instances when it may not be practical. The notice must be available on the website of any dentist who maintains a site [5].

Dentists must use their discretion to make reasonable efforts to limit the use or disclosure of and requests for PHI to the minimum amount necessary to accomplish a particular purpose. This parameter does not pertain to

"certain uses and disclosures including treatment-related exchange of information among health care providers…" [7]. Limiting access to PHI does not mean that the office must be physically redesigned: only reasonable adjustments, such as locked record cabinets and computer passwords, must be implemented. Sign-in sheets are still permitted. Overheard conversations are unavoidable: a dentist needs to take reasonable measures to contain them, such as speaking in low tones. It is expected that when determining the minimum necessary information for an intended purpose, the dentist uses policies and procedures that are practical for the size of the practice [5].

Documented staff training is required by HIPAA to ensure that staff is trained to understand privacy procedures before the compliance date and new members are trained within a reasonable time after hiring. Each staff member must be trained further when changes in policies and procedures result in a change in his or her function. HIPAA does not specify the nature and method of any training [7].

The privacy rule takes into account that many times outside contractors and businesses are necessary to carry out certain health care activities and functions for the dentist. These business associates perform functions or activities, using PHI, on behalf of the dentist. They are not members of the typical dental staff but rather entities, such as accountants, certain software vendors, and consultants, who may have access to PHI. The business associate requirements for HIPAA do not apply to dentists who disclose PHI to other dentists or physicians for treatment purposes [7].

Any dentist who has a business associate must have a written contract with that person stating that the associate will safeguard PHI. The business associate must agree to use the information only for the purposes for which they were engaged by the dentist, to protect the information from misuse, and to provide patients with information about themselves and a history of certain disclosures when necessary. Any breaches must be corrected or the contract must be terminated. The dentist is not liable for privacy infractions of the business associate [7].

Although the patient has rights that must be protected, the dentist has discretionary leeway in many instances with the implementation of the rule. The privacy rule gives the practitioner the flexibility to create his or her own policies and procedures that are suitable for the structure and needs of the practice. Whatever is established simply must follow the framework established by HIPAA. For example, HIPAA requires a privacy official. Rather than appointing a trained privacy official and supporting staff that a hospital may need, a dentist can appoint a staff member as the privacy official. This scalability allows for the protection of a patient's privacy while minimizing the practice's financial burden.

Dentists have until April 14, 2003 to come into compliance with these standards. August 2002 is the anticipated release time for the final version of the privacy rule.

Security

If privacy allows a patient to decide who can view or use his or her health information, security is the means for protecting the patient's health information from unauthorized access and use. The security rule establishes standards to develop and maintain the security of all covered entities' stored, maintained, or transmitted electronic PHI, regardless of format [8]. This security includes the progeny of electronic media, such as a paper printout. Through these standards, the rule also can help protect the integrity of PHI by precluding the potential for fraud [9,10].

Strategies for implementation of the security rule are not based on purely technical solutions; the rule also requires the development of security policies and procedures that influence business practices. As with the privacy rule, the proposed security rule remains flexible in its requirements, allowing the dentist to balance the need to secure data against the risk and cost of doing so [8]. The rule remains technologically neutral to accommodate future advances, and it does not address the extent to which the dentist should implement the specific features [8].

The proposed security rule discusses administrative procedures, physical safeguards, and technical security services and mechanisms that depend on the size and needs of a health care entity. For a small dental practice, these requirements can be relatively simple. An evaluation must identify the actual and potential risks to PHI. A staff person designated as the security officer, a vendor, or a consultant can perform this activity. Policies and procedures that are developed to manage these risks must be reviewed periodically to ensure currency. Using the requirements indicated in the rule [8], the following are examples of possible implementations:

- *A contingency plan in the event of a system failure.* This plan could include back-up floppy disks stored in a second location and an arrangement for use of a back-up personal computer (PC).
- *Personnel security policies and procedures.* These policies document access to PHI and include security awareness training. A small practice may keep track of everyone who uses the computers and what files they may access.
- *Personnel clearance procedures.* These procedures may be addressed with personal and professional reference checks.
- *Security configuration management.* This requirement covers "documentation, hardware/software installation and maintenance review, testing for security features, inventory procedures, security testing, and virus checking" [8]. A vendor or security consultant can assist with this task. Physical features, such as virus-checking software, can be included in the purchase of hardware and software or added as part of a support package.

- *Termination procedures*. The security officer can oversee actions taken upon an employee's termination, such as acquiring keys and changing combinations and passwords.
- *Internal audit*. The PCs software should track all persons who have accessed patient information.
- *Security manual*. This document, available to new employees and used as reference, could include "contingency plans, formal records processing procedures, information access controls (rules for granting access, actual establishment of access, and procedures for modifying such access), security incident procedures (for example, who is to be notified if it appears that medical information has been accessed by an unauthorized party), and training" [8].
- *Physical access safeguards*. These safeguards protect the computers and related equipment from fire and other natural and environmental hazards and from intruders. These safeguards could include locked rooms and cabinets and ensuring that the computers have some degree of separation from the public.
- *Technical security services*. These services help guard data integrity, confidentiality, and availability. This requirement may be addressed by assigning a computer user name and password to each authorized staff member.
- *Internet transmission of PHI*. Encryption provided by commercial software may be used to protect PHI that is transmitted and received via the Internet.

The posting of the final security rule is anticipated for August 2002.

National provider identifier

The following information was gathered from the proposed national provider identifier rule [11].

This proposed rule provides for covered entities a standard for a national provider identifier (NPI) in HIPAA standardized electronic transactions. Currently, providers in business with multiple health care plans possess multiple identification numbers within a single plan or across several plans. Implementation of a NPI should further the efficiency and effectiveness of the health care system via administrative simplification.

The NPI is only a number that provides no additional information, such as the type of provider or the state where he or she is located. Qualitative information is stored in the national provider system. Numbers are assigned to covered entities.

The NPI is used for various reasons, such as an identifier for a dentist in health care transactions and between dentists and other providers. Health care plans will be enabled to coordinate benefits with other health care plans. NPI could be used in electronic patient records to identify dentists and other

practitioners. With its use, HHS can establish a cross-referencing system to investigate fraud and abuse files and other program integrity files.

A system has been suggested to issue NPIs. Organizations known as enumerators have the task of gathering and managing information about each dentist. They procure the number from the national provider system for the dentist. HIPAA-compliant dentists are enumerated before dentists who are not covered entities.

The identity of the enumerators is not known currently, although they could be a federally directed registry or a registry in combination with federal programs (health care plans) and Medicaid state agencies. There is currently no final rule for NPI.

National employer identifier

The National Employer Identifier final rule was published May 31, 2002. This rule was established in response to a need for standard employer identifiers. Employer identification numbers (EIN) that were previously assigned by the Internal Revenue Service as taxpayer identifying numbers for employers have now been adopted as the standard unique employer identifiers [12].

In the past, employers have often been identified on claims, for the enrollment or disenrollment of employees in health care plans, or for the payment of health insurance premiums on behalf of employees. The enrollment transaction is currently the only standard transaction where an EIN is required [12].

Employers are not covered entities. Health plans may, however, "as part of their business arrangements with employers…require employer to use the standard transactions and to provide their EINs for this purpose" [12].

The implementation date for this rule is July 30, 2004.

Summary

HIPAA is generating long-awaited change in the health care world. Administrative, operational, and technical solutions are being created in response to the requirements of HIPAA. The current rules emphasize that the regulations' provisions are scalable and allow all entities, whenever possible, to determine how extensively they will address certain issues. The larger the organization, the more complex the HIPAA strategy must be.

Implementation in a small dental practice requires a simple strategy compared to that of a health care plan or clearinghouse. It still takes time and resources for a dental practice to accommodate the numerous HIPAA requirements, however. Although a dentist may find the rules at HHS Web site or other Internet sites, he or she may wish to rely on vendors, consultants, and the guidance of the ADA and other dental organizations to help implement them.

The dentist also should keep in mind that HIPAA compliance is an evolutionary process; future modifications are necessary. As a result, some of the information contained in this material may not be accurate by the time this issue in printed. Dentists always should consult sources such as the ADA or HHS Web site to procure current HIPAA information.

References

[1] Public law. Health Insurance Portability and Accountability Act of 1996, Public Law No. 104–1191. Available at: http://aspe.hhs.gov/admnsimp/pl104191.htm. Accessed: June 28, 2002.
[2] What is HIPAA? Overview of the legislation: administrative simplification under the Health Insurance Portability and Accountability Act 2001. Available at: http://snip.wedi.org/public/articles/details.cfm?id=18. Accessed: June 28, 2002.
[3] Rules and regulations: health insurance reform. Standards for electronic transactions. 45 CFR Parts 160 and 162. Federal Register 2000;65:50311–72. Available at: http://aspe.hhs.gov/admnsimp/final/txFR.htm. Accessed: June 28, 2002.
[4] What is HIPAA? Transactions and code sets: electronic transaction sets 2001. Available at: http://snip.wedi.org/public/articles/details.cfm?id=20. Accessed: June 28, 2002.
[5] Standards for privacy of individually identifiable health information. 45 CFR Parts 160 and 164. Federal Register 2002;67:14775–815. Available at: http://www.hhs.gov/ocr/hipaa/propmods.txt. Accessed: June 28, 2002.
[6] Office for Civil Rights. Standards for privacy of individually identifiable health information. Available at: http://aspe.hhs.gov/admnsimp/final/pvcguide1.htm. Accessed: June 28, 2002.
[7] Rules and regulations. Standards for privacy of individually identifiable health information. 45 CFR Parts 160 through 164. Federal Register 2000;65:82461–510. Available at: http://aspe.hhs.gov/admnsimp/final/PvcPre01.htm. Accessed: June 28, 2002.
[8] Proposed rules: security and electronic signature standards; Proposed Rule, 45 CFR Part 142. Federal Register 1998;63:43241–80. Available at: http://frwebgate.access.gpo.gov/cgibin/getdoc.cgi?dbname=1998_register&docid=fr12au98-28. Accessed: June 28, 2002.
[9] Rocke S. The war on fraud and its effect on dentistry. J Am Dent Assoc 2000;131:241–5.
[10] Tsang A, Sweet D, Wood RE. Potential for fraudulent use of digital radiography. J Am Dent Assoc 1999;130:325–9.
[11] Proposed rules: national standard health care provider identifier. 45 CFR Part 142. Federal Register 2002;63:25320–57. Available at: http://aspe.hhs.gov/admnsimp/nprm/npinprm.txt. Accessed: July 1, 2002.
[12] Rules and regulations. Health insurance reform: standard unique employer identifier. Final rule, 45 CFR Parts 160 and 162. Federal Register 2002;67:38009–20. Available at: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2002_register&docid=02-13616-filed.pdf. Accessed: June 28, 2002.