the Journal of CONTEMPORARY DENTAL PRACTICE at www.thejcdp.com
Volume 4 Number 1 February 15, 2003 Winter Issue

The Health Insurance Portability & Accountability Act and the Practice of Dentistry in the United States: Privacy and Confidentiality

Joseph E. Chasteen, DDS, MA; Gretchen Murphy, MA
Arden Forrey, PhD; David Heid, DDS

Abstract

This paper introduces the reader to the Health Insurance Portability and Accountability Act (HIPAA) of 1996 legislation in the context of its relationship to the Electronic Oral Health Record (EOHR). Privacy and confidentiality issues for administrative data are addressed in terms of the broader relationship of such data to the EOHR leaving the HIPAA-defined administrative transactions and security issues for the entire practice for a subsequent presentation. Educational requirements are presented that aid the dentist and the practice staff in understanding the broad and long-term implications of the HIPAA legislation.

Keywords: Health Insurance Portability and Accountability Act, HIPAA, privacy

Citation: Chasteen JE, Murphy G, Forrey A, et.al. The Health Insurance Portability & Accountability Act: Practice of Dentistry in the United States: Privacy and Confidentiality. J Contemp Dent Pract 2003 February;(4)1:059-070.

Introduction

President Clinton signed the Health Insurance Portability and Accountability Act (HIPAA) of 1996 on August 21, 1996 as Public Law 104-191. The intent of the Administrative Simplification sections of this law is to create a mandatory format (messages and code sets) to be used by any healthcare entity like a dental office that transmits health information in an electronic transaction and to protect the confidentiality and security of health information by setting and enforcing standards.[1] While HIPAA addresses only one part of the information management problem in healthcare, it was the first targeted step in creating effective recognition of the role of information coupled with the use of information science and technology in healthcare. Figure 1 depicts the inextricably linked realities of information in healthcare. The first domain deals with patient care issues presented by Heid, et al.[2] This paper and its sequel deal primarily with the resource management information domain, but this portion focuses on the privacy and confidentiality issues. The ultimate goal is to expedite the exchange of healthcare data in a confidential and efficient manner that results in a reduction in administrative costs associated with the management of such information.

Figure 1. Domain Inseparability

The law also applies to all health plans and healthcare clearinghouses. Clearinghouses are organizations that receive messages in a noncompliant form and reformat them into a different form that is compliant with the provisions of HIPAA.

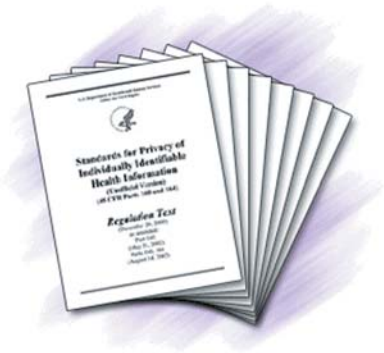
Heid, et al. provided an overview of the significance of the Electronic Health Record (EOHR) to the dentist and noted there are a number of Electronic Data Interchange (EDI) transactions that are potentially relevant to the dental practice.[2] The most relevant is the Healthcare Claim (Transaction 837 Dental) that contains those attributes from the EOHR that characterize the dental encounter or patient visit and the services rendered. The key attributes are extracted from the EOHR by appropriately designed software and automatically assembled into the HIPAA-designated message form that includes other attributes denoting the healthcare insurance coverage and enrollment information.

Should a dentist or a health plan elect not to use the required electronic standard to transmit patient information electronically, HIPAA provides for the use of a clearinghouse that is compliant with the standard for such transmissions. Since paper transactions are not subject to HIPAA regulations, they can be used to submit information between businesses such as the dental office and a health plan as in the past without additional requirements.[3]

In order to achieve the intent of the law, the following elements are included in the regulations:

1. All patient health data used in the administrative transactions, as well as the associated administrative and financial data, must be standardized.
2. Unique identifiers for patients, employers, health plans, and healthcare providers, such as dentists, must be implemented.
3. Privacy and security standards for computer systems designed to protect the confidentiality and integrity of "individually identifiable health information" must also be implemented.
4. Electronic signature standards must be in place.

The HIPAA rules do not offer preemption requirements. The HIPAA privacy rule is a "floor" for privacy protection. This means that more stringent state laws superseded HIPAA and states have a right to apply for HIPAA exception for existing or new state laws when conflict or stringency is uncertain. Dentists will need to be sure their practices conform to both HIPAA rules and specific state laws that apply. For example, an individual state may have more stringent privacy requirements for mental health information. Keep in mind that dentists may continue to respond to public health mandatory reporting requirements.



Several papers[4,5] and informational sources[6] have also addressed the meaning of HIPAA for the dentist. The objective of this report is to further describe the key patient care data that is captured in the EOHR with that used for administrative functions. For an integrated dental practice enterprise, the view of the additional resource management data needed for complete practice management will be depicted. The primary emphasis of HIPAA is twofold: (1) protecting personal health information and (2) standardizing transactional data. Each of these will be addressed in this paper. In addition, a discussion will be presented of how EOHR information architectures for dental practices should be designed for transparent, consistent use of patient care data used for the administrative functions that are now the focus of the HIPAA legislation.

Protecting Personal Health Information (PHI)

The HIPAA privacy rule is designed to protect a patient's personal health information from being accessed by an unauthorized person. The privacy rule actually builds on well-accepted principles for patient privacy and dovetails with state laws as well as institutional policies for handling protected health information. April 14, 2003 is the target date for the privacy rules to be in place.

Still, the HIPAA rule lays out a new privacy environment for patients and for healthcare providers. More consumer control over health information is called for in the following ways:

1. Patients are to be informed in more detail about the use of their protected health information at the beginning of their care by receiving a notice of privacy practices document prepared by the provider or healthcare organization.
2. Patients are given the right to examine and obtain a copy of their health records and are allowed to amend the records if errors have been made and if they follow a written process to make such amendments. Exceptions are allowed in special cases such as when access to the information may be harmful to the patient.
3. Written authorizations from patients are required for the release of their health information; they may revoke authorizations if they wish. Authorizations are not required in cases where release is required by law.
4. Patients may request their providers to provide an accounting of their health information disclosures made in the six years prior to the request. This accounting extends only to protect health information that was disclosed to entities outside the organization. According to the HIPAA rule, patients do not have a right to know who has seen their records in the course of providing care or billing activities.[7] However, it is important to check with individual state law in the area of patient's rights.
5. If privacy violations occur, patients may file a complaint regarding the violations at the provider level and with the Secretary of Health and Human Services with the assurance there will be no retaliation against the patient.

For healthcare providers including dentists, the privacy rule sets boundaries on the use and release of health information. With few exceptions, health information is to be used for healthcare and related purposes. The rule also requires providers establish clear privacy policies and procedures. For example, privacy procedures should describe how patients are to authorize the release of their protected health information and should specify that, when disclosing health information, providers limit the release to the "minimum reasonably needed" for the purpose of the disclosure.

Dentists must therefore establish clear privacy policies and procedures for privacy practices. A privacy officer is required to oversee the privacy practices to assure that appropriate policies and procedures are adopted and followed. In small practices, an office manager may serve in this capacity along with other business responsibilities. In larger organizations, the privacy officer focuses entirely on the privacy requirements, developing policies and procedures, and overseeing related activities.

The rule lays out a new privacy environment for patients and for healthcare providers. The HIPAA privacy rule gives patients more control over their health information. Patients will be informed in more detail about the use of their protected health information at the beginning of their care, and they have a specific opportunity to learn about how their information is used. They also are given the right to examine and obtain a copy of their health records and may amend the records if errors have been made. Patients' written authorization for the release of their health information is clearly defined and their rights to revoke authorizations are spelled out. Patients may receive an accounting of their health information disclosures from their providers. Finally, patients may file a complaint regarding privacy violations at the provider level and with the Secretary of Health and Human Services with no retaliation against the patient. Many of these features of the privacy rule are already in place in healthcare settings today. Typically, patients are asked to sign authorizations to disclose their health information; in many states, patients have the right to receive copies of their health record.

The privacy rule calls for privacy training for all staff, but the training component may be setting aside an opportunity to review the privacy policies and procedures with the small staff so the review should be conducted before starting training.

There are numerous HIPAA aids available online and Samples of Notice of Information Practices documents can be found at http://www.ahima.org/journal/pb01.05.3.htm as well as other sites.

The HIPAA privacy rule sets a national floor for minimum privacy standards. Some states have stronger laws providing additional privacy protection. This means that individual providers must be sure their policies and procedures accommodate both the HIPAA requirements and those of applicable state laws. The privacy rule also accommodates existing public health mandatory reporting requirements.

Privacy Policies

The privacy rule clearly defines civil and criminal penalties for privacy violations and, by doing so, strengthens the patchwork privacy protections currently available throughout the United States. For example, privacy procedures should describe how patients are to authorize the release of their protected health information. Authorizations are required for releasing information to insurance companies for payment and for other special release of information. Existing policies on confidentiality of health information will serve as a basis and may be modified to include HIPAA specific language. The recent American Dental Association's (ADA) publication "HIPAA Privacy Kit" features an overview of policies and procedures for dental practices that offers suggestions on how to achieve HIPAA compliance and features examples and illustrations that may be adapted.[7]

While state laws may vary, for HIPAA the rule calls for privacy policies to include at least the following elements:

1. A general statement prohibiting the use and disclosure of patients' protected health information without authorization or otherwise permitted by law and noting that only the minimum necessary information will be disclosed when authorized.
   - Authorizations for use and disclsure– their use and the form to be used. (Authorization examples are available in the ADA HIPAA Privacy Kit[7], p. 69)
   - Authorizations from other providers
2. Provision for notifying patients of the privacy practices of the dental office, the availability of the notice document along with patient acknowledgements they have received the notice, and that the notice will be displayed in the public areas of the office.
3. Provision for patient access to their record for purposes of review and/or amendment, paper or computer review Amendment procedures, and the form patients use to request an amendment to their record.
   - Denial of access - cases where the provider (dentist) refuses access along with an example
4. Opt Out policies such as if patients do not want to have their information used for specific things.

5. Sanctions for privacy breaches – from verbal correction to termination of staff.
6. Complaint process (including language that assures there will be no retaliation against patients who file complaints) and forms for the patient to use.
7. An accounting of disclosures that explains how HIPAA requirements for the accounting applies in the dental practice.

Professional Communications and Privacy

The HIPAA rule certainly allows the necessary communication among members of the healthcare team for care purposes or for billing purposes. However, when disclosing health information to others, such as insurance companies, providers are required to limit the release to the **"minimum reasonably needed"** for the purpose of the disclosure. The law generally prohibits disclosure of protected health information unless the patient authorizes it. This prohibition includes a restriction on re-disclosure of health information that has been provided from another provider. Updated policies and procedures must specify this. This means the minimum necessary requirement does not apply among staff in the dental office in the ordinary course of caring for patients.

Even small dental practices are required to give their patients a "Notice of Information Practices" document, which informs patients about their privacy rights and explains how their health information will be used for treatment, payment, and healthcare operations. The notice must contain the following items specified in Figure 2.

A sample notice is also provided on page 61 of the HIPAA Privacy Kit[7] published by the ADA. Adjustments may be required where state law plays a role.

Patient Authorization Requirements

While patient authorization is required for the use and/or disclosure of their protected health information, authorizations are not required to disclose such information to the persons or agencies listed in Table 1.

Accounting for Disclosures

When responding to a patient's request for an accounting of the disclosures of their protected health information, providers must comply within 60 days. Note this accounting applies to the

Sample Patient Notice

This notice describes how information about you may be used and disclosed and how you can get access to this information. Please review it carefully.

This dental practice will handle your patient care information to ensure privacy although treatment information with other providers and payment claim transactions will not require your authorization for each instance. Any changes in these policies will be given to you either during appointments or by mail.

However, if the practice is involved in any clinical research trial or other non-routine treatment practice that may require conveying information from your patient care record to other practitioners, you will be asked to authorize or deny such information sharing.

You have the right to see all information recorded in your record and make copies of it. You may request amendment of any incorrect information.

This practitioner recognizes responsibility for protecting the privacy of all patient care information in this practice, as defined in PL 104-191 (1996) <and any additional state requirements>. Any concerns may be reported to <the appropriate State Agency> at < at address and phone>. The person to contact in this practice regarding any questions or amendments is <Dr X> at <practice phone number>.

<Practitioner Name and Current Date>

"designated record set." The designated record set must be specified in the policies and procedures. For providers, it will include the following items:

- The legal medical record
- Billing and claim information
- Remittance information
- Eligibility and claim status responses
- Charge screen information
- Statement of account balance
- The payment agreement

It also includes consent and authorization forms, Medicare LifeTime Reserve Letter, Medicare Notice of Non-Coverage Letter, and a copy of the insurance care. These may be stored in separate locations. The designated record set should not include administrative data such as quality reviews.[8]

Privacy Training

The privacy rule calls for privacy training for all staff. In a dental practice, the training component may be setting aside an opportunity to review the privacy policies and procedures with the staff. Periodic review of privacy practices can be done at annual review periods and when changes in practice affect how business is conducted. There are a number of vendor HIPAA training programs available that may be selected for staff to attend. Online training options are also becoming available.

Business Associate Agreements

Business Associate Agreements need to stipulate that privacy practices adhere to the HIPAA rule. Where business associates release protected

Figure 2. Notice of Practices

Right to notice header that states:

This notice describes how information about a patient may be used and disclosed and how a patient can get access to this information. Please review it carefully.

Content of Notice:

- A description of the uses and disclosures the provider expects to make without individual authorization including examples of treatment, payment, and healthcare operations.
- Statements indicating the provider will use and disclose the information in other ways with the patient's authorization and the patient can revoke the authorization.
- Descriptions of patients' rights to request restrictions, inspect, and copy protected health information; amend or correct protected health information; and receive an accounting of disclosures.
- Statements about the provider's legal requirements to protect privacy, provide notice, and adhere to the notice.
- An explanation of how the provider will inform individuals about changes to its policies and procedures.
- Instructions on how to complain to the entity or the Department of Health and Human Services.
- Name and telephone number of a contact person or office.
- Date the notice was produced.

Provision of Notice:

Providers must provide the notice to all patients at the beginning of care, on request of the patient, and whenever changes in practices occur. Best practice is to provide a copy of the notice to the patient and ask the patient note they have received the notice.

See http://www.ahima.org/journal/pb01.05.3.htm as well

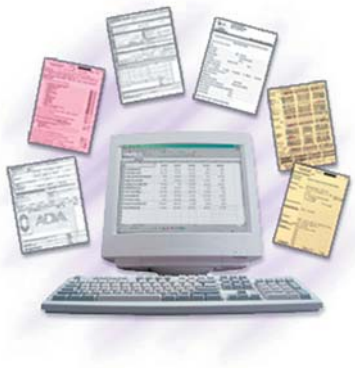
Table 1.

- The patient
- Family and designated friends
- Public health authorities
- Child abuse and neglect reporting
- Food and Drug Administration reporting
- Communicable disease reporting
- Workplace safety
- Victims of abuse, neglect, or domestic violence
- The judicial and administrative proceedings
- Law enforcement
- Deceased patient
- Research in accordance with institutional review board oversight; de-identified health information (patient identifiers removed) is recommended whenever there is a possible serious threat to health or safety
- Specialized government functions such as national security
- Coroners and medical examiners

health information, they must be able to respond to individual patient's requests for a record of accounting. Dental offices need business associate agreements in the form of written contracts that specify the business associate will safeguard and limit their use of protected health information.

Educational Requirements

The educational aspects of HIPAA are just the beginning of a much more substantial effort that will be needed by all healthcare professional disciplines, including dentistry, to understand the implications of electronic information management in healthcare. The first steps involving HIPAA will be directed at abstraction of those data from the patient care record that characterize administrative steps. Claims and payment are only one of these steps. The dentist needs to understand how these steps will fit together in the information architecture that will be centered on the EOHR and the challenge will be to provide various levels of education that show the general informational mosaic while, for the present, focusing on the HIPAA-mandated administrative steps. Once these steps are mastered using present records and information systems, the pathway to the full EOHR environment discussed in the earlier article and the pathways to acquisition and use of EOHR systems can be better appreciated. Education will also need to touch on the supply chain issues because the same software message handling tools that deal with the HIPAA transactions can be configured to manage practice inventory and reorder of supplies in a much more transparent fashion. Suppliers in healthcare are already positioning themselves for this transition and it will eliminate staff time spent on this quite well understood but time-consuming process. It will require the dentist to understand for his/her practice how these functions are to be organized. Thus, the education process needs to recognize this.



An Overview of HIPAA and its Dental Implications

The reality is that before HIPAA, all participants would not recognize, and then invest in the necessary information science and technology to deal with, the prime role of information in integrally managing the two perspectives of patient care and resource management. In dentistry the emphasis has been on "practice management", i.e., resource management, but like the rest of healthcare, it was driven from the fragmented, paper record perspective of historic activities that embraced resource management rather than support of patient care. Even following the 1991 Institute of

Medicine landmark report[11] for the United States, resources were not directed to the needed changes that were identified in this report. The Clinton Administration, following the election of 1992, attempted a major restructuring of healthcare financing. These efforts foundered on the differences between unilateral and multilateral payment organizations schemes, but they made abundantly clear the plethora of data constellations, vocabularies, and classification schemes that were used to characterize healthcare resource management and payment processing. This recognition led to concerted work on "Administrative Simplification" of the federally funded healthcare programs, fully recognizing the common conventions adopted would apply across all such activity. Because the activities addressed were primarily commercial, the care conventions were to be based on those standards that have already been introduced into regular commercial use by the Data Interchange Standards Association (DISA) in the US, the United Nations Electronic Data Interchange For Administration, Commerce and Transportation (UN-EDIFACT), and the International Standards Organization (ISO). There were certain differences in approach that are now being harmonized to a single conceptual framework.

The impact on handling health information was aided by the approach of the World Wide Web communications architecture and technology that showed the advantages of a unified approach. The PL-104-191 of 18 August 1996 recognized these administrative data management steps were precursors to, and facilitators of, the vision of the 1991 IOM report for the EHR capability. The recent 2001 Institute of Medicine report "Crossing the Quality Chasm" clearly states the need to follow the Administrative Simplification steps with those that tie these initial functions into an information environment that supports the integrated achievement of both patient care and resource management functions in ways that lead to a demonstrably quality healthcare system. The challenge now is to understand not only why this is so but also what health information knowledge and skills that oral health practitioners will need to master the role that these two key perspectives contribute synergistically to promoting effective oral health patient care. Effective resource management will enable patient access to care and that access, when coupled with more effective care, will lead to healthcare applications having proportionally less drain on resources for maintaining that health status.

As was noted in the earlier paper[7], training of personnel will be an ongoing process, especially because dentistry will become part of various healthcare teams, such as in the care of diabetic patients or other chronic health conditions with an oral health component. Most training is focused on particular psychomotor skills but it will need to be coordinated with the educational activities that will build the broader perspective. This coordinated approach will benefit the dentist because as the healthcare system undergoes the changes anticipated by the IOM, the practice staff will have from their experience with the HIPAA administrative transactions a more resilient view of the change process.

One of the aspects that will be part of the HIPAA transition, as well as part of the healthcare evolution to embrace the quality care principles stated by the 2001 IOM report, is dentists will be involved as participants in care teams with increased communication with patients and their education about their individual involvement in oral health practices attending all health conditions. The first steps in this communication will start with HIPAA.

Staying Current with the Regulations

Despite the burden of other aspects of managing a dental practice, the dentist needs to keep an eye on the evolutionary trajectory of information technology that supports the practice. There is an ongoing introduction of products and services to aid the dentist, but each practitioner needs to continue to evaluate them in terms of the functions that link support of patient care to the administrative transactions needed to communicate with the world external to the practice as well as help internal practice management. The ADA's website (www.ada.org) and the work of the ADA's Standards Committee on Dental Informatics (SCDI) is, as was noted earlier[2], an important central source of focused information for the dentist. Numerous informational websites will arise and some of these will also appear on the general EHR website http://www.ehrweb.org, also noted earlier. These sites will provide links to other specialty sites such as those relevant to the dental practice supply chain, specialty services, training, and other professional education subjects that can be accessed from the present and future practice information architecture using the common hardware and software infrastructure of the practice. The outlook developed by the dentist in complying with the HIPAA requirements addressed in this presentation will enable this ability.

Conclusion

The compliance deadline for the "Transactions Regulation" governing the transmission of healthcare was October 16, 2002. However, there has since been a provision for extending that compliance deadline for one year. The compliance deadline for the "privacy rule" protecting the confidentiality and integrity of health data will become effective April 14, 2003, unless proposed modifications in this regulation are adopted and the date is subsequently altered.

The HIPAA regulation imposes severe civil and criminal penalties for non-compliance. These include:

- Fines up to $25,000 for repeated violations of the same standard within a calendar year.
- Fines up to $250,000 and/or imprisonment up to 10 years for knowing misuse of individually identifiable health information.

Recognizing the severity of the consequences for non-compliance, it behooves the dentist to take the necessary steps to achieve compliance. These steps will include:

1. Establishing awareness of HIPAA requirements in the dental office.
2. Comprehensive assessment of the office information security systems, policies, and procedures.
3. Creating an action plan for compliance with deadlines and timetables for compliance. A comprehensive action plan should include:
   - Developing new policies, processes, and procedures for handling healthcare information
   - Building "Chain of Trust" Agreements with billing services to assure compliance
   - Designing a compliant technical information infrastructure within the office
   - Purchasing new, or adapting, information systems when appropriate
   - Developing new internal communication strategies to avoid breaching patient confidentiality
   - Staff training on HIPAA requirements
   - Implementation of enforcement policies and procedures

References

1. HIPAA Primer. Phoenix Health Systems web site: http://www.hipaadvisory.com/regs/HIPAAprimer1.htm
2. Heid DW, Chasteen J, Forrey AW. The Electronic Oral Health Record". J Contemp Dent Pract. 2002 Feb 15;3(1):43-54.
3. American Dental Association web site: http://www.ada.org/prof/prac/issues/topics/hipaa/index.html
4. Pai SS, Zimmerman JL. Health Insurance Portability and Accountability Act (HIPAA). Implications for dental practice. Dent Today. 2002 Oct;21(10):106-11; quiz 111, 178. No abstract available.
5. Walker RJ. "HIPAA Strategy for Dental Schools" J Dent Educ. 2002 May;66(5):624-33.
6. Health Information Compliance Insider, Brownstone Publishers, Inc. June, 2002.
7. HIPAA Privacy Kit, American Dental Association 2002.
8. Amatayakul, M., "What's Your Designated Record Set?, HIPAA on the Job." J AHIMA. 2002 Jun;73(6): 16A-16C. No abstract available.
9. HIPAA Administrative Simplification, Proposed Security Rule (l998) http://aspe.os.dhhs.gov/admnsimp/bannerps.htm#security
10. Phoenix Health Systems web site: E-mail Transmissions http://www.hipaadvisory.com/alert/vol1/vol1num9.htm#new
11. Dick RS, Steen EB, Detmer DB "The Computer-based Patient Record – An Essential Technology for Healthcare" Revised Edition Washington DC National Academy Press 1997.

About the Authors

Joseph E. Chasteen, DDS, MA

Dr. Chasteen is an Associate Professor in the Department of Oral Medicine at the University of Washington School of Dentistry and serves as the Director of Infomation Technology and Research.

Gretchen Murphy, MA

Gretchen F. Murphy Med, RHIA is Director and Senior Lecturer of the Health Information Administration Program, School of Public Health and Community Medicine at the University of Washington in Seattle, WA. She has represented the American Health Information Management Association in several health informatics standards activities and chaired the ASTM Technical Committee on Health Informatics' Subcommittee on the Structure and Content of the Electronic Health Record from 1992-2002. She has authored several books and book chapters on health information management subjects.

Arden Forrey, PhD

Dr. Forrey serves as a Research Associate in the Department of Restorative Dentistry, University of Washington School of Dentistry. He has served as the Veteran's Administration Decentralized Hospital Computer Project Site Manager at the Seattle VA Medical Center; a Research Fellow in Fleet Medical Informatics, US Navy Medical Research and Development Command, and in the Department of Pediatrics at Georgetown University.

David Heid, DDS

Dr. Heid is the former Chief of Dental Services at the Seattle Veterans Medical Center in Seattle, WA and now serves as a Clinical Professor in the Department of Restorative Dentistry at the University of Washington School of Dentistry. He has also held the position of an Associate Professor in the Department Restorative Dentistry at the Medical College of Georgia.

e-mail: dheid@cablespeed.com