HIPAA Overview

The Health Insurance Portability and Accountability Act (HIPAA) was signed into law August 21, 1996. This landmark legislation affects nearly everyone involved in the healthcare process from providers to healthcare information systems vendors to payers. HIPAA contains provisions for the portability of insurance coverage as employees move from one employer to another. It also contains provisions for Administrative Simplification covering the privacy and security of individually identifiable healthcare information and for government-mandated Standards for electronic Transactions, Code Sets and Identifiers. HIPAA Administrative Simplification provisions require the protection of patient-identifiable data from inappropriate disclosure and define the type of information that must be protected and the circumstances under which this information can be disclosed. HIPAA Administrative Simplification Security provisions define the policies, analyses, practices, and mechanisms that must be conducted or put in place to ensure that the privacy of “protected health information” (PHI) is maintained. The goals of the Administrative Simplification provisions are to improve the efficiency and effectiveness of healthcare through standardization of all shared electronic PHI, protect the confidentiality of PHI stored and exchanged electronically and reduce the cost of exchanging PHI among healthcare partners. HIPAA Administrative Simplification establishes standards for the format and data content of various healthcare transactions. It also sets minimum requirements for the transmission, storage and handling of healthcare information. Organizations governed by HIPAA rules, or "covered entities," include all health plans, all healthcare clearinghouses and those healthcare providers who transmit healthcare information electronically for the purposes identified under the HIPAA Transaction Standards.

The Privacy Rule

The Privacy Rule applies to "individually-identifiable health information" transmitted or stored in any form (paper, oral, or electronic) that concerns an individual's past, present, or future physical or mental health, or that relates to the provision of health care to or payment of health care for the individual. The phrase "individually-identifiable health information" refers to any health-related information that could be used to identify an individual. Examples include but are not limited to the following:

- Names
- IP addresses
- Addresses
- Certificate numbers
- Cities and countries
- License numbers
- Phone numbers
- Zip codes
- Fax numbers
- Account numbers
- Email addresses
- Birth dates
- Web addresses
- Comparable Images

Patients are afforded a number of rights under the Privacy Rule, including the right to adequate notice of privacy policies, the right to access PHI, the right to an accounting of disclosures, and the right to request amendment of PHI. Covered entities are obligated to implement a number of administrative requirements (including privacy initiatives, security administration and physical and technical security safeguards for PHI) in order to honor these patient rights and achieve compliance with the other provisions of the Rule. Covered entities are generally permitted to disclose PHI to "business associates," provided that they obtain written contractual assurances from each business associate that it will safeguard the information.

HIPAA Overview
(cont.)

A business association is created when the right to use or disclose information belongs to the covered entity and another party requires the information either (1) to perform a function for or on behalf of the covered entity (e.g. billing or practice management services) or (2) to provide certain specified services (e.g., legal and accounting) to the covered entity. A business associate contract is not required in very limited circumstances – for example, where a disclosure is made for treatment purposes from one provider to another.

Carestream Health may be the business associate of a customer who qualifies as a covered entity when selected products and services are provided and is committed to safeguarding any PHI we may receive in connection with such products and services. Carestream Health can provide a Business Associate Agreement upon request.

The HIPAA statute establishes a range of civil and criminal penalties for violation of the Privacy Rule. HHS has emphasized that the Privacy Rule is intended to be "scalable" so that they can be implemented reasonably and appropriately with a broad range of covered entities from single-provider dental and physician practices to national hospital chains. HHS' Office for Civil Rights (OCR) has been charged with enforcing the Privacy Rule.

The Transaction Standards

The HIPAA Administrative Simplification provisions also include government-mandated Transaction Standards for electronic data Interchange (EDI).

The electronic transactions covered by those Standards include the following:

- Healthcare claims or equivalent encounter information;
- Eligibility for a health plan
- Referral certification and authorization
- Healthcare claim status
- Enrollment and dis-enrollment in a health plan
- Healthcare payment and remittance advice
- First report of injury
- Health plan premium payments
- Coordination of benefits

The rules with respect to the HIPAA Transaction Standards define a distinctive role for healthcare “clearinghouses,” allowing them to provide services to translate non-compliant data into standard electronic formats (ANSI X12). The PracticeWorks Electronic Services clearinghouse, which directly handles transactions for a large percentage of our dental clients, has purchased and integrated translation software into its clearinghouse operations to convert non-compliant transactions into compliant transactions as provided under HIPAA regulations. This clearinghouse service is particularly important to our existing practice management dental clients, since it provides a mechanism for them to meet the HIPAA Transaction Standards without a substantial investment in software or hardware upgrades.

The PracticeWorks Electronic Services clearinghouse has been certified by an independent testing facility (Claredi) as HIPAA compliant for claim transactions. See details by clicking on the icon on the right. This means that our customers using PracticeWorks Electronic Services as instructed can send electronic transactions covered by the HIPAA Transaction Standards and be considered compliant under the Standards.

HIPAA Overview
(cont.)

The American Dental Association (ADA) is one of the Designated Standards Maintenance Organizations (DSMO) for HIPAA. DSMOs are organizations identified to maintain the standards for healthcare transactions adopted by the Secretary of HHS, and to receive and process requests for adopting a new standard or modifying an adopted standard. The ADA is responsible for maintaining the CDT-4 and future code sets (Dental Procedure Codes), and makes recommendations for changes to the Transaction Standards to accommodate specific dental requirements. The ADA web site also provides assistance to dental practices in understanding HIPAA requirements.

The Security Rule

The Security Rule includes provisions for Security Administration, Physical Security and Technical Security Services and Mechanisms designed to protect the confidentiality, integrity and availability of electronic protected health information (E-PHI). The Rule is composed of a set of required security standards that must be met, and another set of addressable standards. Addressable standards must either be strictly enforced, or an analysis of alternative enforcement provision mechanisms must be available to substantiate implementation by other means.

In all cases, our customers must begin by performing a security assessment of their entire enterprise in order to uncover risks that may threaten the E-PHI they processes, and the vulnerabilities to these threats within their information technology systems. Thereafter, specific controls required to comply with the Security Rule must be interwoven into their operational and information management systems and into those of their business associates by April 2005.

Conclusion

Only through employee training, operating procedures and the information processing tools and services provided by Carestream Health and/or similar vendors will healthcare providers have the ability to comply with HIPAA. Our customers should note that there are no specific requirements posed by the Privacy Rule, Transaction Standards or Security Rule that mandate any particular software mechanism or functionality; however, it is clear that many customers will have to upgrade existing software and make operational changes to enable their systems and end users to become HIPAA compliant.