

The HIPAA Security Rule became effective on April 20, 2005. For our customers that believe they need an amendment to their existing Business Associate Agreement with Carestream Dental to incorporate additional HIPAA Security language, we have prepared such an Amendment that is available here. Simply print the Amendment, which has already been executed by Carestream Dental, and mail it to us. For additional information on HIPAA Security, please see below.

Carestream Health's Perspective on Healthcare Privacy and Security

Carestream Health Imaging is committed to developing and delivering services and products that assist and enable our customers to comply with privacy and security regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the Privacy Directive (EU 95/46 EC) in Europe. The goal of these regulations is to improve the efficiency of healthcare administration while ensuring the privacy, confidentiality and security of patient-identifiable health information. Compliance with these regulations requires providers and payers to review operational practices, modify administrative policy and process, and apply technology. Carestream Health is committed to delivering services and products that assist our customers in achieving these goals.

The HIPAA Legislation Title 2 of HIPAA, Administrative Simplification, is designed to improve the efficiency of healthcare by standardizing electronic transactions, protecting the privacy of individually identifiable patient information and requiring that specific security analyses and technologies are used or considered toward protection of electronic versions of protected health information. The purpose of the legislation is to make electronic exchange of information between health plans and healthcare providers easier, and therefore less costly, over the long run. Congress, however, recognized that the collection, use, storage and exchange of individually identifiable patient information needed to be managed in ways that would preserve a patient's right to privacy. The rules governing privacy have been enforceable since April 2003; the security rules will be enforceable in April 2005, and both are monitored by the U.S. Department of Health and Human Services (HHS). Details on the HIPAA Privacy rule and the HIPAA Security rule can be found on the HHS Administrative Simplification web page.

Our customers and Carestream Health understand that the HIPAA regulations stress "reasonable and appropriate" measures be used to address a covered entity's privacy, security and business policies and requirements. For this reason, specific administrative and technical needs will vary for each enterprise based upon the specifics of how the enterprise operates and the patients it serves. In order to protect patient data, healthcare providers must assess their patient health information collection, use and disclosure processes, and security practices as well as the automated systems they employ and procedures they follow. Then, if compliance gaps are identified, our customers will have to remediate those gaps violating the Privacy Rule immediately and those gaps violating the Security Rule by April 2005.

Carestream Health's Imaging Products and Services Are Being Readied

Carestream Health is dedicated to quality. We are committed to supplying our customers with best in-class imaging products, information systems and services that enable them to comply with all legal and regulatory requirements. We encourage each of our customers to gain an understanding of the privacy and security regulations that govern their enterprises such as HIPAA in the USA, evaluate the impact of such regulations on their operations and prepare their organizations to be compliant. It is important to understand that software, hardware or services from Carestream Health or any other vendor (other than clearinghouse services) cannot be "HIPAA-compliant," nor can privacy or security

optimized products confer that status for the user. Systems and services can, however, provide tools to assist a healthcare professional in meeting its compliance requirements.

With respect to clearinghouse services, the Carestream Dental Electronic Services clearinghouse has been certified by an independent testing facility (Claredi) as HIPAA compliant for claim transactions. In support of Radiology and other medical and dental practices, Carestream Health Imaging has released Privacy-Enabled products and services that help our customers meet the patient privacy and security obligations they face by automating the performance of important services. Such products and services include those related to confidentiality, integrity, individual accountability, emergency access and other key requirements. In addition, dental customers using the Carestream Dental Electronic Services clearinghouse can rely on the clearinghouse's third-party certification to meet any HIPAA requirements applicable to claims submitted electronically.

Carestream Health Imaging Group has an assigned Privacy/Security Officer to coordinate, educate and manage our efforts in this arena. Carestream Health is also a leader in and a participant with industry trade groups and standards bodies, including the Joint NEMA (National Electrical Manufacturers Association)/COCIR (European Coordination Committee of the Radiological and Electromedical Industry)/JIRA (Japan Industries Association of Radiological Systems) Security and Privacy Committee, Working Group 14 -- Security of the DICOM (Digital Imaging and Communications in Medicine) Standards Community, and the HIMSS Medical Device Security and Privacy Working Group. As always, Carestream Health customers can count on our dedication to provide products and services that work in concert with their own administrative security policies, procedures and training. The combination of sound processes and procedures, coupled with new Privacy-Enabled Carestream Health information technology and services, can assist customers in meeting the privacy and security challenges they face with HIPAA in the USA, and related regulations in all other regions of the globe.

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
- Addresses
- Cities and countries
- Phone numbers
- Fax numbers
- Email addresses
- Web addresses (URLs)
- IP addresses
- Certificate numbers
- License numbers
- Zip codes
- Account numbers
- Birth dates
- 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. 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; and
- 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 Carestream Dental 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 Carestream Dental 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 Carestream Dental Electronic Services as instructed can send electronic transactions covered by the HIPAA Transaction Standards and be considered compliant under the Standards.

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.