HIPAA and the COD: Background and Introduction

HIPAA
Other national sites of interest can be found at the bottom of this document.

University Organizational Environment
The University of Iowa is a “Hybrid Entity” of which the College of Dentistry is a component. Debbie Thoman is the University HIPAA Privacy Officer and Jane Drews is the University IT Security Officer. The University provides certain University level controls such as policies, procedures, and resources. University resources include:
HIPAA at the UI: [http://itsecurity.uiowa.edu/hipaa/](http://itsecurity.uiowa.edu/hipaa/)
IT Security : [http://itsecurity.uiowa.edu/](http://itsecurity.uiowa.edu/)
UI Healthcare: [https://www.uihealthcare.org/patientrights/](https://www.uihealthcare.org/patientrights/)

In reference to the above diagram, Transactions and Identifiers refer to the business process and the identifiers, procedure coding standards, and rules that are required to effect portability and administrative simplification. Dental Informatics and the Business
Office are primarily responsible for awareness and implementing these regulations. Privacy policies and procedures and compliance requirements are the most visible aspects of HIPAA. Documentation related to the HIPAA Privacy Rule at the University of Iowa can be found at [http://itsecurity.uiowa.edu/hipaa/](http://itsecurity.uiowa.edu/hipaa/) Clinic Administration is primarily responsible for privacy compliance. These three components require security in order to function. Security compliance is primarily Dental Informatics responsibility.

**Security**

IT security procedures and best practices are a set of procedures established by various vendor and business and groups. IT security is a dynamic process with constantly changing threats, technologies, and business demands. The University and the college have long implemented security policies and procedures as needed to maintain the quality and operational continuity of their respective operations. Various collegiate and university business operations require IT security, healthcare being but one of them.

HIPAA security relies upon this pre-existing function and requires risk remediation controls to be compliant with best practices targeting ePHI. The Final HIPAA Security Rule mandates a much more structured and documented process, thus as a byproduct will affect and improve other aspects of institutional IT management. IT security is an ongoing process, not a destination.

The Security Rule contains the following concerning security and privacy:

“As many commentators recognized, 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. It is important that we note several distinct differences between the Privacy Rule and the Security Rule.

The security standards below define administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic protected health information. The standards require covered entities to implement basic safeguards to protect electronic protected health information from unauthorized access, alteration, deletion, and transmission. The Privacy Rule, by contrast, sets standards for how protected health information should be controlled by setting forth what uses and disclosures are authorized or required and what rights patients have with respect to their health information.”

While the security rule does not address paper based PHI security, the privacy rule requires security for all PHI. Due to the extreme difficulty of managing and monitoring security and privacy for paper based records, HIPAA compliance creates a significant motivation to transition toward more secure and manageable electronic record keeping systems.

**IT Security Management**

Changes in threats, technology, and IT utilization effect risk. The goal of IT security management is to reduce the risk of loss of confidentiality, loss of data integrity, and loss of availability (operational continuity). The following are recommended phases for on-
going security management. These steps are developed for compliance of the Final HIPAA Security Rule of April 21, 2005.

The process for continual IT security management will involve a process similar to the following:

**Working Towards HIPAA “Compliance” -- A Certification Process**

- Gap and Risk Analysis
- Policy and Technical Infrastructures
- Ongoing Monitoring and Evaluation
- Education and Awareness

*Diagram concept from HIPAA: A Real World Approach to Compliance – HIMSS 2001 Conference*
Repository of HIPAA Awareness Documents

The enterprise has created and maintained a repository of HIPAA awareness documents and has updated the repository based on periodic checks of the key HIPAA Internet sites, including:

HIPAA websites


(d) "http://www.hhs.gov/news" (HHS press releases on HIPAA)

(e) “http://aspe.dhhs.gov/adminsimp” (HHS Administrative Simplification website)

(f) "http://www.privacysecuritynetwork.com"


(h) "http://www.hipaa-dsmo.org/" (Designated Standard Maintenance Organizations; FAQ's and procedures for requesting a change)

(i) "http://www.hl7.org/" (Accredited Standards Developer chartered by ANSI)

(j) "http://www.healthprivacy.org/" (Health Privacy Forum website, containing compendium of state privacy laws)

(k) "http://www.ahima.org" (American Health Information Management Association; benchmark case studies)

(l) "http://www.aha.org/advocacy-issues/hipaa/index.shtml” (listing of current HIPAA articles)

(m) “http://www.hipaagives.org” (HIPAA web-site for states)

(n) “http://www.hcpro.com” (HIPAA training and other materials)