

HIPAASuccess - Physician Education Series

Legislative Background

Your Faculty: Walt Culbertson

- President and Founder, Connecting Healthcare®
- Host and Producer, Medical Update Show
- Served as Technical and Operations Lead, HIE Project Manager Florida Health Information Exchange
- Served as the State of Florida Technical SME for the ONC State Health Policy Consortium, Southeast Regional HIT-HIE Collaboration (SERCH)
- Founding Executive Director, ePrescribe Florida and President, ePrescribe America
- Founding Chair of the Southern Healthcare Administrative Regional Process (SHARP), a regional collaborative workgroup alliance of private and public health care organizations and HHS, HRSA and CMS
- Founding Co-Chair of the CMS Sponsored Southern Insurance Commissioner Task
 Force, a regional collaborative workgroup alliance for State-level HIPAA Education
- Founding Security and Privacy Co-Chair for the Workgroup for Electronic Data Interchange (WEDi) Strategic National Implementation Process (SNIP)



Why HIPAA?

 Health Care delivery has evolved to require enormous administrative efforts across many organizations

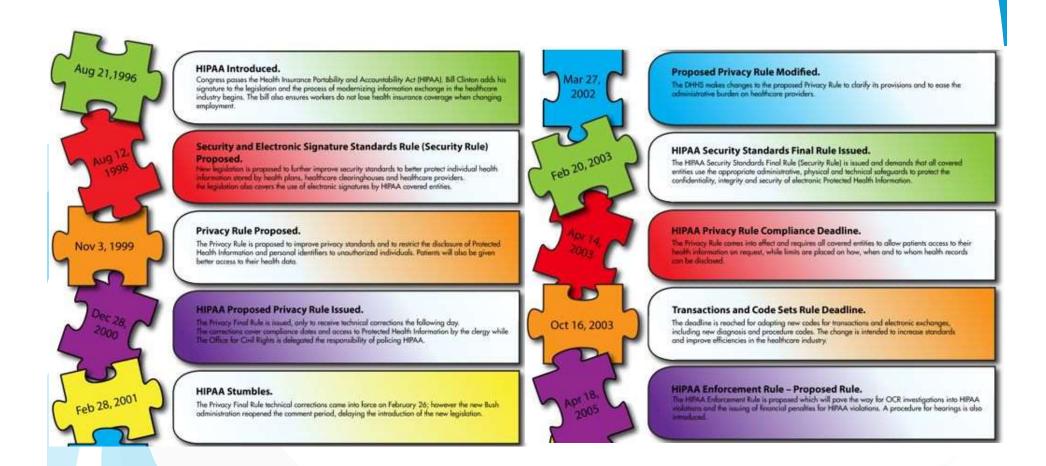


What is HIPAA?

- Health Insurance Portability and
 - Accountability Act
 - Congress passed law in 1996
 - Kennedy and Kasselbaum co-sponsored bill
 - First provisions finalized concerned portability of health care coverage

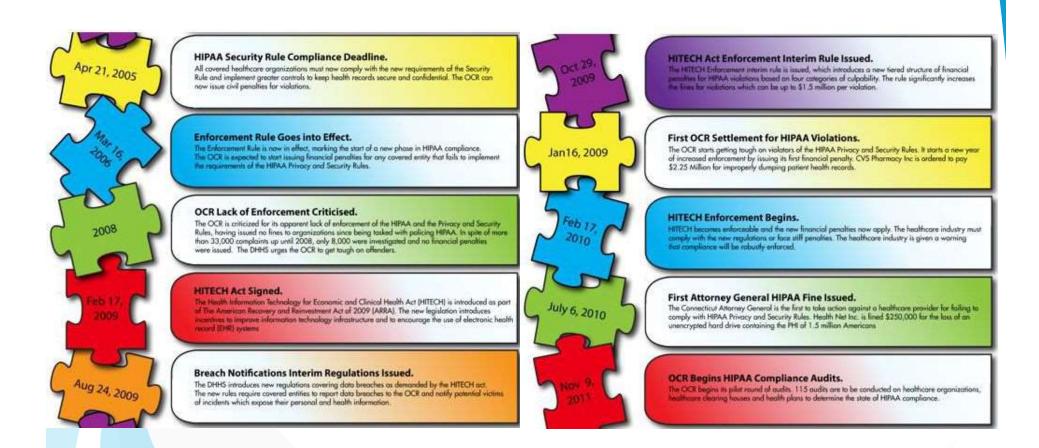


History of HIPAA Timeline 1996 - 2005





History of HIPAA Timeline 2005 - 2011





History of HIPAA Timeline 2012 - 2015



Omnibus Final Rule Finalised.

The Madifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules is received for review by the Whitehouse Office of Management and Budget. The long awaited changes include a number of provisions of HITECH and involve major updates to HIPAA

OCR Compliance Pilot Audits End.

The first round of compliance audits comes to an end revealing the poor state of HIPAA compliance. The healthcare industry has been slow to introduce the new changes required by the Privacy

HIPAA Omnibus Final Rule Issued.

The DHHS releases the Omnibus Final Rule which incorporates the changes to HIPAA demanded by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009. The new rule makes sweeping changes to improve data security, further restrict access to eFHI, prevent the use of PHI for marketing and the Enforcement Rule is also enhanced.

Omnibus Rule Comes into Force.

The Omnibus Rule takes effect and all HIPAA-covered entities must now comply with the new legislation. The healthcare industry is given six months to camply before the rule will be enforced.

The new legislation also updates breach notification rules and Business Associates can now be

wild liable for breaches and certain HIPAA violations

Technical Corrections to the Omnibus Rule.

The comment period allowed covered entities and the public to vaice concerns about the new Omnibus Rule, and the DHHS decides to make minor corrections to improve workability of the bill, by improving flexibility and decreasing the burned on covered entities.



Omnibus Rule Compliance Deadline.

The Omnibus Final Rule becomes enforceable and all covered entities, which now include business associates and their contractors, must obide by the new rule or face a financial penalty of up to LS million per violution. The Omnibus Rule, Security Rule and Privacy Rule are to be assessed in the accord round of 400 HIFAA compliance audits scheduled for late 2014.

HIPAA Audits Delayed until 2015.

The OCR announces it will be delaying its second round audits to allow it to test its new web portal system The new web portal will be used to report data breaches and collate audit paperwork.

This year the OCR is due to complete the delayed second round of HIPAA compliance audits, which are espected to prese the way for a permanent HIPAA compliance audit program. Here technology and ever more determined and resourceful hackers are sure to see HIPAA continue to each in acide to maintain high standards of security in the healthcare industry.



HIPAA Origin and Intent

- HIPAA was designed to:
 - Protect health insurance coverage for workers and their families when they change or lose their jobs
 - Prevent discrimination against employees and their families due to existing medical conditions



HIPAA Origin and Intent

- In trying to address these challenges, it became clear that Healthcare must standardize certain data:
 - Core Business Interactions and Code Sets used within the transactions
 - Key Identifiers such as the:
 - Patient identifier
 - Health plan identifier
 - Employer Identifier
 - Provider Identifier

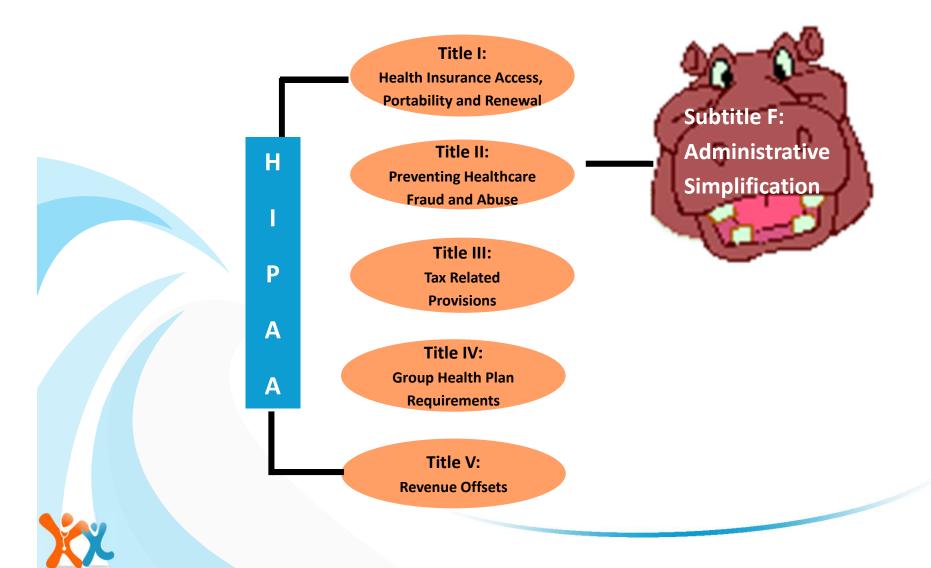


HIPAA Origin and Intent

- Also become clear that data must be securely and confidentially shared between insurers and providers
- This lead to rules being promulgated for:
 - Privacy
 - Security



HIPAA Components



HIPAA Provisions

- Group and Individual Insurance Reform
 - Portability of coverage, guaranteed issue and renewal
 - Limits on pre-existing exclusion provisions
- Tax-Related Health Provisions
 - Managed Spending Account (MSAs)
 - Long-term care insurance
 - Taxation of insurance benefits



HIPAA Provisions

- Fraud and Abuse
 - Medicare integrity, data collection, beneficiary incentive programs
 - Increased penalties, sanctions, and exclusions
 - Administrative Simplification (AS)



HIPAA Regulatory Process

The Department of Health and Human Services (DHHS) issues the regulations

- Publishes proposed rule in Federal Register
- Provides mechanisms for public comment
 - Usually 60 day time period
 - Reviews comments and revises rule



HIPAA Regulatory Process

DHHS Publishes final rule in Federal Register & notifies Congress

- Rule effective 60 days later (Final Comment Period)
- Mandatory compliance 24 months later (36 months for small plans with less than \$5 million in annual revenue)



Standards Maintenance Process

- Transactions maintained by industry groups
 - Establishes a new category of organization, The Designated Standard Maintenance Organization (DSMO)
 - Memorandum of Understanding from six organizations
 - Web site: http://www.hipaa-dsmo.org



Standards Maintenance Process

- Code sets maintained by owners
- Annual Review/Update Process
 - Public input
 - National Committee on Vital and Health
 Statistics
 - Regulations as needed



Penalties and Fines

Non-Compliance with Requirements

\$100 per violation to a maximum of
\$25,000 per requirement per year

 The security rules contain many specific requirements and the addressing the application of HIPAA penalties



Penalties and Fines



- Wrongful Disclosure of Health Information
 - Simple disclosure fines up to\$50,000 and/or one year in prison
 - Disclosure under false pretenses fines up to \$100,000 and/or five years in prison
 - Disclosure with intent to sell or use fines up to \$250,000 and/or 10 years in prison

Assess All HIPAA Provisions

- While they were released in a staggered fashion, the HIPAA regulations are interdependent within the systems and operations of covered entities
- None of the provisions of Administration Simplification should be assessed nor remediated in a vacuum
- Later releases of the final rules will further effect changes already in progress as well as implemented solutions to meet earlier specifications



Remember - HIPAA is Not the only Law

- Issues will exist over preemption floor/ceiling
- Since HIPAA does not preempt all state laws, then HIPAA is not the only law of the land
- HIPAA preempts all contrary state laws, except where state laws are "more stringent" than HIPAA
- Explore industry standards. Assess how HIPAA will interplay with state requirements, focus on procedural issues for privacy and security policies and procedures



Gramm Leach Bliley

GLB Act provides protection for:

- Non-public personal information about individuals who obtain financial products or services for personal, family or household purposes
- Covers financial information not health care information



Gramm Leach Bliley Definition

Non-public Personal Information

- Includes any personally identifiable financial information provided by a customer or consumer to a financial institution to obtain a financial product or service
- Financial institution includes insurance companies and health plans



Gramm Leach Bliley Quick Summary

What GLB allows:

- Sharing of information with "affiliated" companies
- Sharing of information with "non-affiliated" companies ONLY following
 - Notice of a company's information sharing practices
 AND
 - Providing an opportunity to customers to "opt out" of disclosures



Gramm Leach Bliley Who is covered?

- Financial institutions including insurance companies and health plans
 - State insurance authorities will enforce GLB for insurance companies and health plans – need to monitor laws in states where conduct business
 - DHHS: GLB may fall under HIPAA clauses regarding preemption – comply with GLB now and worry about preemption later



Gramm Leach Bliley When?

Compliance Date: July 1, 2001

- Some states have requirements that must meet prior to this date
- Cannot disclose information to non-affiliated companies unless have previously provided
 - Notice of disclosures
 - Allowed 30 day period following notice for individuals to "opt out" of disclosures



Gramm Leach Bliley What to Do?

- Conduct privacy audit
 - What financial information do you currently share with whom?
- Issue privacy notice
 - Allow time for individuals to opt out
- Modify systems to
 - Track "opt out" elections of individuals
 - Protect against unauthorized disclosure of nonpublic personal information







Have Questions?

Visit our Website, send us an email, or give us a call!

(904) 435-3456 (904) 435-3457 (904) 435-3457 (Questions@ ConnectingHealthcare.com

