

An Executive Overview

**Health Insurance Portability & Accountability Act of 1996
"HIPAA"**

***U.S. Public Law 104-191
HIPAA Administrative Simplification
Title II, Subtitle F***

***Second National Medical Banking Institute
March 26, 2003
Washington, DC***

***Presented by Rachel Foerster & Associates, Ltd.
Beach Park, IL 60099
www.rfa-edi.com
Course HC-006a***

RACHEL FOERSTER & ASSOCIATES, LTD.
Professionals in EPI & Electronic Commerce

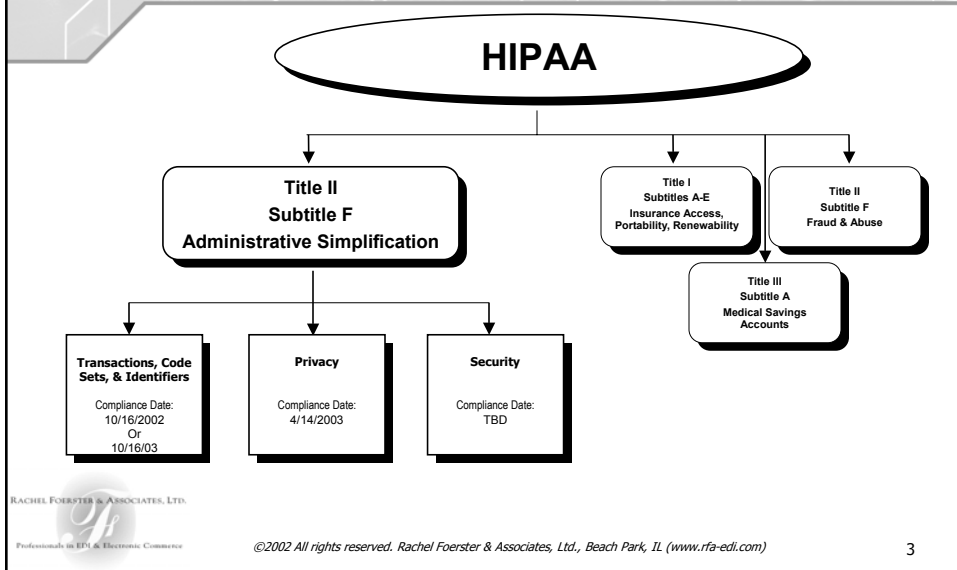
What is HIPAA?

- ***HIPAA . . . A Federal Law Created in 1996***

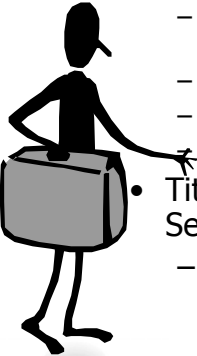
<u>H</u>	=	<u>H</u>health
<u>I</u>	=	<u>I</u>nsurance
<u>P</u>	=	<u>P</u>ortability &
<u>A</u>	=	<u>A</u>ccountability
<u>A</u>	=	<u>A</u>ct

RACHEL FOERSTER & ASSOCIATES, LTD.
Professionals in EPI & Electronic Commerce

HIPAA Overview



Insurance Reform



- Amends the Internal Revenue Code of 1986 to
 - Improve portability and continuity of health insurance coverage in the group and individual markets
 - Combat waste, fraud, and abuse in health insurance and health care delivery
 - Promote the use of medical savings accounts
 - Improve access to long-term care services and coverage
 - Other purposes
- Title II, Subtitle F amends Title XI of the Social Security Act to
 - Improve Medicare, Medicaid, overall health care system
 - Simplify the administration of health insurance

RACHEL FOERSTER & ASSOCIATES, LTD.
Professionals in EPI & Electronic Commerce

©2002 All rights reserved. Rachel Foerster & Associates, Ltd., Beach Park, IL (www.rfa-edl.com)

4

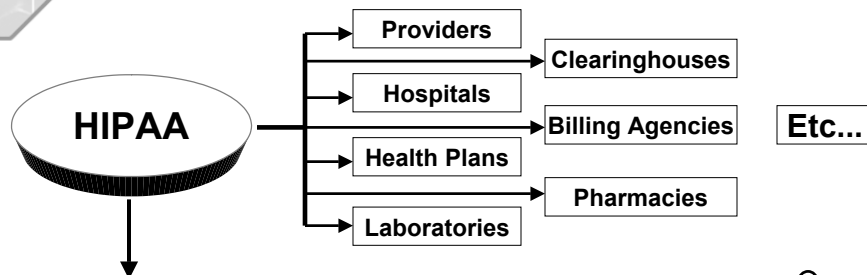
Administrative Simplification

- Improve the efficiency and effectiveness of the healthcare system by standardizing electronic transmission of certain health care TRANSACTIONS



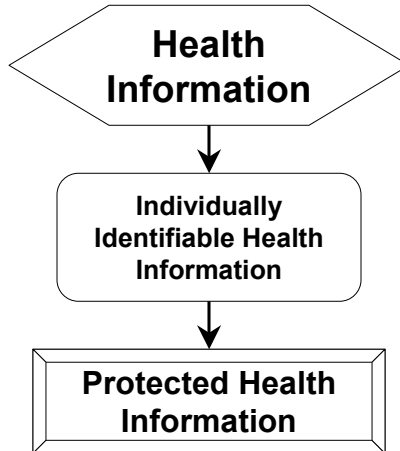
- Protect the PRIVACY and SECURITY of all health care information (including transmitted information)

Who Is Affected?



Indirect Applicability: All organizations that exchange data with those directly covered under the HIPAA through Business Associate Agreements or Chain of Trust Agreements

Definitions: Health Information



Health Information: Definitions

- **Health information** means any information, whether oral or recorded in any form or medium, that:
- (1) Is **created or received** by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
- (2) **Relates** to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Health Information: Definitions

- **Individually identifiable health information** is information that is a subset of health information, including demographic information collected from an individual, and:
 - (1) Is **created or received** by a health care provider, health plan, employer, or health care clearinghouse; and
 - (2) **Relates to** the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
 - (i) That **identifies the individual**; or
 - (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual

Health Information: Definitions

- **Protected health information** means individually identifiable health information:
 - (1) Except as provided in paragraph (2) of this definition, that is:
 - (i) Transmitted by electronic media;
 - (ii) Maintained in any medium described in the definition of electronic media at § 162.103 of this subchapter; or
 - (iii) Transmitted or maintained in any other form or medium.
 - (2) **Protected health information excludes** individually identifiable health information in:
 - (i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
 - (ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and
 - (iii) Employment records held by a covered entity in its role as employer.

Unique Entities

Clearinghouse

Processes health information received from another entity in nonstandard format or containing nonstandard data content into standard data elements or standard transaction

Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity

Business Associate

On behalf of a covered entity performs, or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information where the provision of the service involves the disclosure of individually identifiable health information from the covered entity or from another business associate of a covered entity

A clearinghouse is prohibited from using or disclosing protected health information other than as permitted in the business associate contract under which it created or received the protected health information

Healthcare Clearinghouse

- *Health care clearinghouse* means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and “value-added” networks and switches, that does either of the following functions:
 - (1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.
 - (2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Indirect Applicability – Business Associate

- *Business associate*: (1) Except as provided in paragraph (2) of this definition, *business associate* means, with respect to a covered entity, a person who:
 - (i) On behalf of such covered entity or of an organized health care arrangement (as defined in § 164.501 of this subchapter) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of:
 - (A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or
 - (B) Any other function or activity regulated by this subchapter; or

Indirect Applicability – Business Associate

- (ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.
- (i) A covered entity may disclose protected health information to a business associate and may allow a business associate to create or receive protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information.

Business Associate Agreement

- A Business Associate Contract is NOT required¹
 - When a financial institution processes consumer-conducted financial transactions by debit, credit, or other payment card, clears checks, initiates or processes electronic funds transfers, or conducts any other activity that directly facilitates or effects the transfer of funds for payment for health care or health plan premiums
 - When it conducts these activities, the financial institution is providing its normal banking or other financial transaction services to its customers; it is not performing a function or activity for, or on behalf of, the covered entity
 - With a person or organization that acts merely as a conduit for protected health information, for example, the US Postal Service, certain private couriers, and their electronic equivalents

¹OCR HIPAA Privacy Guidance, December 3, 2002

What If You Do Not Comply?

Non-Compliance (Civil Penalty)

- \$100 for each violation
- Maximum of \$25,000 per year per incident

Unauthorized Disclosure or Misuse of Patient Information (Criminal Penalty)

- ◆ Penalties up to \$250,000
- ◆ Prison time up to 10 years

Penalties may apply to the individual violator but they may also apply to the organization or even to its officers

Enforcement

PRIVACY CIVIL PENALTIES:

The OFFICE OF CIVIL RIGHTS (OCR) within the Department of Health and Human Services (HHS) will enforce the civil penalties

PRIVACY CRIMINAL PENALTIES:

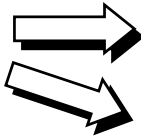
THE DEPARTMENT OF JUSTICE will enforce the criminal penalties

ELECTRONIC TRANSACTIONS, CODES SETS

The CENTER FOR MEDICARE & MEDICARE SERVICES (SMC) within the Department of Health and Human Services (HHS) will enforce the civil penalties

HIPAA's Impact

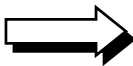
OPERATIONAL:



Administrative and Clinical Procedures
(EXAMPLE: Billing, Operations, Coding, Claims Processing)

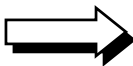
BAA Contracts and/or COT Agreements
(EXAMPLE: Providers, Payers, Clearinghouses, other healthcare service companies)

MANAGERIAL:



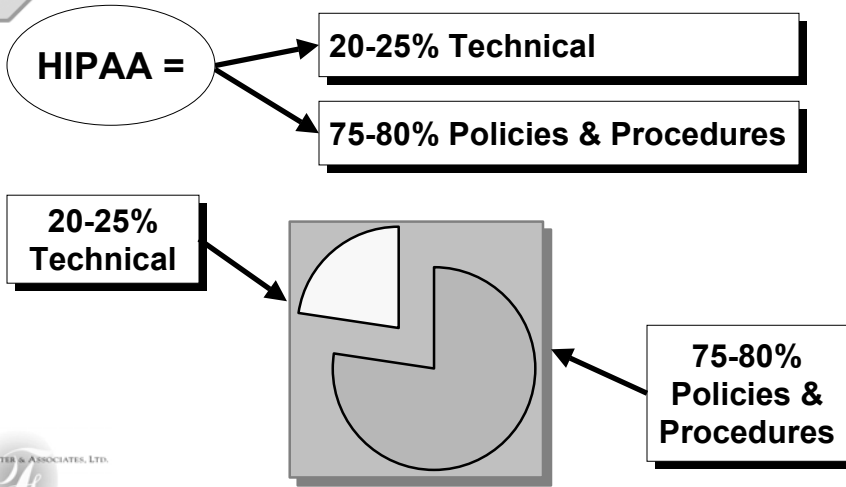
- Leadership & Support
- New or Revised Policies

TECHNOLOGICAL:

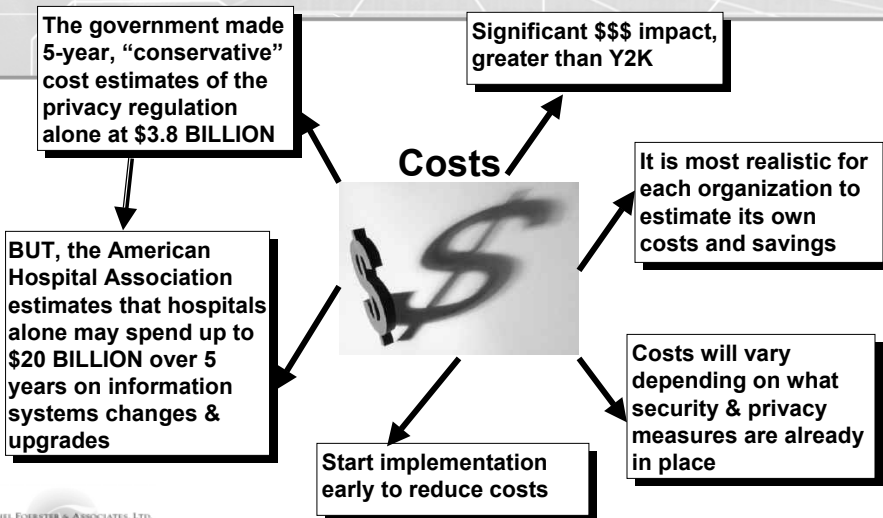


- Interoperability (Hardware, Software, Connectivity)
- Security Infrastructure
- Vendor Management

HIPAA's Impact



Costs



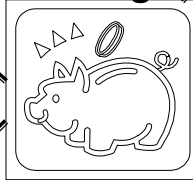
Savings

The health care industry estimates that full implementation of these provisions could save up to \$9 billion per year from administrative overhead without reducing the amount or quality of health care services

Costs associated with mailing, faxing, & telephoning will decrease

A PAPER-based claim costs \$6.00 to \$8.00 to process... The same claim in ELECTRONIC form costs \$0.17 to process

Savings



Hospitals will no longer have high costs associated with the development of customized systems solutions

Transactions will become more standardized, resulting in eventual savings for electronic data interchange... Claims received without key entry (electronic transaction) and payments made without paper & check saves money

Currently, an average of \$0.26 of each health care dollar is spent on administrative overhead (enrolling in health plan, paying health insurance premiums, processing claims, etc.)

Privacy Vs. Security

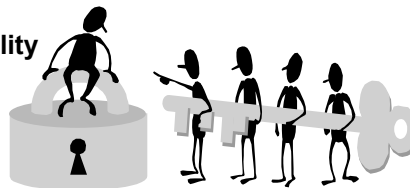
➤ Privacy

Refers to **WHAT** is protected — Health information about an individual and the determination of WHO is permitted to use, disclose, or access the information

➤ Security

Refers to **HOW** private information is safeguarded — Ensuring privacy by controlling access to information and protecting it from inappropriate disclosure and accidental or intentional destruction or loss

C = Confidentiality
I = Integrity
A = Access



**You cannot have
Privacy without
Security**

Privacy

PRIVACY COMPLIANCE DATE = April 14, 2003

- HIPAA privacy regulation is applicable to:
 - Covered Entities — Healthcare Providers, Health Plans, and Clearinghouses
 - Protected Health Information (PHI) — Individual (Patient) identifiable information relating to the past, present or future health condition of the individual transmitted or maintained in any form or medium (includes paper and oral)
 - Floor of Provisions — Does not preempt more stringent state laws, potentially requiring some dual systems

What Does the Privacy Rule Mean?

◆ Limits the **Use** and **Disclosure** of Health Information

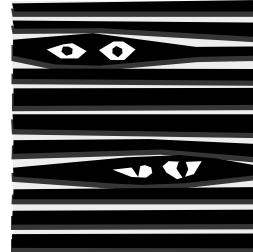
Use = Employment, application, utilization, examination, or analysis of information **WITHIN** an entity that holds the information

Disclosure = Release, transfer, provision of access to, or divulging in any other manner of information **OUTSIDE** the entity holding the information

- ### ◆ Establishes Individual's (Patient's) right to access and use of health information
- Right to inspect or copy health information
 - Right to amend incorrect information
 - Right to receive an accounting of all disclosures made for reasons *other than payment, treatment, or health care operations*

What Does the Privacy Rule Mean?

- Balances health information protection and individual rights against public health and safety needs
- Administrative Requirements
 - Privacy Officer
 - Patient Notice
 - Training for **ALL** Employees
 - Sanctions
 - Documented Policies & Procedures



Privacy Impacts

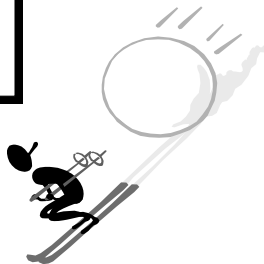
Extensive business unit involvement will be necessary to develop policies & procedures consistent with regulations

Technical and physical security infrastructure must be assessed to insure safeguards to protect health information are adequate

Initial and on-going training initiatives will be required

Business Associate Agreements must be reviewed & modified to incorporate privacy protections

Policies and procedures must be strictly enforced to avoid penalties up to \$250,000 and prison time up to 10 years



Security

Purpose:

To protect both the system and the information it contains from unauthorized access & misuse

Encompasses:

All safeguards in a covered entity's structure including:

- Information systems (hardware/software)
- Personnel policies
- Information practice policies
- Disaster preparedness

SECURITY → FINAL RULE PUBLISHED 2/20/03

Very few changes from proposed rule

More in sync with Privacy

More clearly identifies "required" vs "addressable"

Security

Administrative Procedures

To ensure security plans, policies, procedures, training, and contractual agreements exist

Physical Safeguards

To provide assigned security responsibility and controls over all media and devices

Technical Security Services

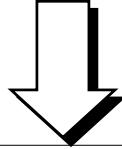
To provide specific authentication, authorization, access, & audit controls to prevent improper access to electronically stored information

Technical Security Mechanisms

To establish communications/network controls to avoid the risk of interception and/or alteration during electronic transmission of information

A Final Comment on Privacy & Security

The privacy and security rules are flexible & scalable to account for the nature of each organization's culture, size, resources.



Each organization will determine its own privacy policies & security practices within the context of the HIPAA requirements & its own capabilities, needs & tolerance for risk.

Transactions & Code Sets

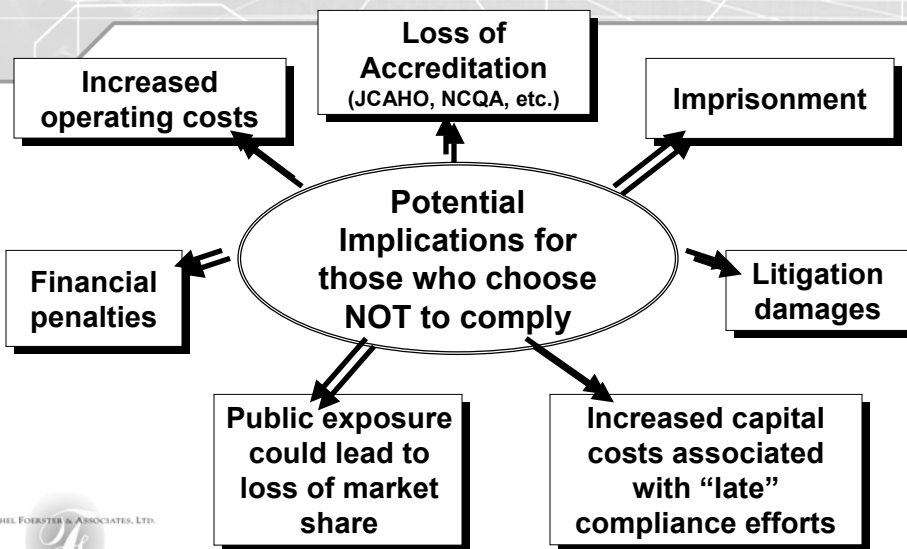
**TRANSACTION COMPLIANCE DATE =
October 16, 2002 else
October 16, 2003 if you filed an ASCA Extension
Includes Addenda**

You must use the standard transactions and code sets if you conduct your business electronically.

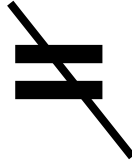
Milestones & Compliance Dates

HIPAA Section	Issue Date	Compliance Date						
		10/16/02	4/14/03	10/16/03	4/14/04	7/31/04	4/21/05	
Transactions & Code Sets								
Small health plans	8/17/00	●	
Extension granted (if requested)	8/17/00			●	
Addenda (includes relaxation of NDC & Provider Taxonomy codes, replacement of NCPDP formats with 835 for retail pharmacy claims payments)	12/27/01			●	
Testing of Transactions	2/20/03				●	
	12/27/01		●	
Privacy								
Small Health Plans	12/28/00		●	
Modifications to Final Rule	8/14/02				●	
	8/14/02				●	
Security								
Small Health Plans (additional year to come into compliance: 4/21/06)	2/20/03						●	
Unique Health Identifiers								
Employer ID	7/30/02						●	
Provider ID	TBD						
Health Plan ID	TBD						
Individual ID	Unlikely						

Non-Compliance Implication



HIPAA Compliance



Administrative Simplification

HIPAA Compliance

**HIPAA is
NOT
an IT Project**

Administrative Simplification

Contact Information

RACHEL FOERSTER & ASSOCIATES, LTD.

Professionals in Health Care EDI, Privacy & Security

RACHEL FOERSTER, CEO & PRESIDENT

39432 North Avenue, Beach Park, IL 60099-3602

Voice: 847.872.8070 Fax: 847.872.6860

E-mail: rachel@rfa-edi.com

<http://www.rfa-edi.com>

RACHEL FOERSTER & ASSOCIATES, LTD.

Professionals in EDI & Electronic Commerce

©2002 All rights reserved. Rachel Foerster & Associates, Ltd., Beach Park, IL (www.rfa-edi.com)

35