

Re-engineering Health Care

Coping with HIPAA's Administrative Simplification Regulations

Presented by:

Holt Anderson, Executive Director, NCHICA

The Program

- **HIPAA Overview**
- **Transactions, Codes & Identifiers**
- **Security**
- **Privacy**
- **Compliance Strategies & Tools**

HIPAA

Health Insurance Portability & Accountability Act of
1996 [PL 104-191]

- Administrative Simplification
 - **Electronic Transactions & Codes**
 - National Identifiers
 - Security [& Electronic Signatures]
 - **Privacy**
- Compliance deadlines beginning in Oct 2002
- Civil Monetary & Criminal Penalties

HIPAA VS Y2K?

- Not a “one shot deal”
- Not solely a technology or systems fix
- Not an easy “return to normal operations”
- Affects much more than technology

Wishful thinking about HIPAA

- Congress will repeal HIPAA
- HIPAA is a Clinton program; with a new President, it will go away
- There will be no HIPAA enforcement for many, many years
- My vendor will take care of HIPAA
- HIPAA is an IT project

The Major (likely) Benefits for Typical Provider

- Reduce staff in business office and registration
- Reduce IS support for interface engine and EDI communication
- Reduce staff that manage enrollment, referral, and eligibility by phone and paper
- Collect most accounts at time of service; health plan and sponsor payments within ten days

The Major (likely) Benefits (cont)

- Reduce bad debt
- One-time A/R gain of up to \$100K per physician
- Protection of your information resources
- Standard security/privacy policies and procedures
- Est. savings of \$18K per FTE physician per year

What is Missing?

- Individual identifiers
- One set of privacy rules with state preemption
- Medical records information standards
- Resources to implement the standards

What is Missing? (cont)

- HIPAA enforcement (regulation pending)
 - Office of Civil Rights (will do Privacy)
 - Justice Department
 - FBI
 - Lessons learned from Fraud & Abuse
 - Will accreditation reviews be an effective enforcer?

*** FINAL RULE ***

**ELECTRONIC TRANSACTIONS
& CODE SETS**

October 16, 2002

Transactions & Codes

Objective: Standardize EDI transactions, reduce handling and processing to achieve efficiency and savings.

⇒ **Challenges:**

⇒ *There are about 400 formats for electronic health claims in use today.*

⇒ *Elimination of local codes will require renegotiation of contracts.*

Transactions & Codes

What is the Rule?

- Standards for financial and administrative transactions, data elements, and codes for those transactions, to enable health information to be exchanged electronically

Covered Entities

- Health Care Providers
- Health Care Clearinghouses
- Health Plans
- [Business Associates]

Transactions & Codes When?

- Published in Federal Register August 17, 2000
- Became effective October 16, 2000
- Implemented by October 16, 2002 or monetary penalties may apply

Transactions

	<u>ASC X12N</u>
Enrollment/Dis-enrollment:	834
[Invoice	811]
Premium Payment:	820
Eligibility Request & Response:	270/271
Authorization/Certification, Request & Response:	278
Claim or Encounter:	837
Claim Status Inquiry & Response:	276/277
Payment and Remittance:	835

Standardized Code Sets

- **ICD-9-CM** (diagnosis & procedures)
- **CPT-4** (services of physicians, other professionals)
- **HCPCS** (products, supplies & services)
- **CDT** (dental services)
- **NDC** (Rx drugs in pharmacy transactions)

Local Codes



Rules Pending

- [Coordination of Benefits Transactions - 837]
“ Health Plans are only required to accept COB transactions from other entities, ... with which they have trading partner agreements to conduct COB.”
- [Claims Attachments]

Implementation Considerations

- Migration from Current to New Process
- Operational Impacts
 - Constraints
 - Opportunities
- Resource Considerations

Developing Your Plan

- Identify transactions that must or could be migrated
- Evaluate use of Health Care Clearinghouses
- Inventory all systems that send or receive transactions
- Question current vendors about their plans
- Develop your organization's approach to compliance
- Establish timing and sequence of testing with business partners
- Determine conversion issues
- Agree on timetable

*** PROPOSED RULE ***

UNIQUE IDENTIFIERS

National Identifiers

- Providers
- Health Plans
- Employers
- Individuals [deferred indefinitely]

*** PROPOSED RULE ***
SECURITY

Objective

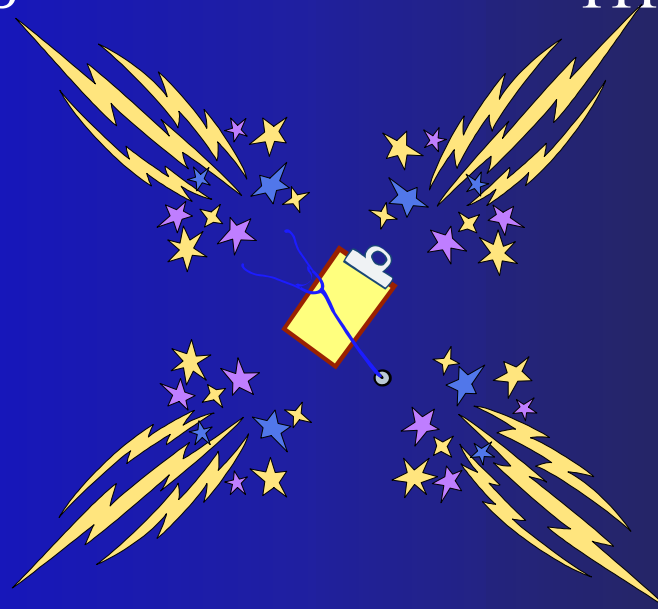
- Maintain data integrity, confidentiality and availability

⇒ *Challenge: Think beyond just HIPAA to an effective security program for your entire organization*

SECURITY THREATS

TARGETED
THREATS

RANDOM
THREATS



HUMAN
NATURE

ACTS
OF GOD

Security NPRM Requirements Review

Administrative

Certification
Chain of Trust
Agreements
Contingency Plan
Formal Mechanisms:
Records
Info Access Control
Internal Audit
Personnel Security
Security Configuration
Security Incident
Procedures
Security Mgmt.
Process
Termination
Procedures
Training

Physical Safeguards

Assigned Security
Responsibility
Media Controls
Physical Access Controls
Policy - Workstation Use
Secure Workstation
Location
Security Awareness
Training

Electronic Signature

Digital Signature
Expected to be removed
from final rule

Technical Security Mechanisms

Communications/Network
Controls
Integrity Controls
Message Authentication

Technical Security Services

Access Controls
Audit Controls
Authorization Controls
Data Authentication
(corruption)
Entity Authentication

Look at Implementation Features Under Each Requirement

Risk Assessment

- Required to be performed:
 - Identify security threats and vulnerabilities
 - Develop, implement & maintain safeguards to protect such data
 - Must be documented
 - Meet HIPAA Security Rule requirements
 - Balance of costs vs. risks
- ⇒ *Integrate Privacy Regulations & Other Compliance Requirements in Assessment*

Risk Management Methodology

- Identify potential areas of loss, in terms of money, information, or reputation
- Identify threats
- Identify vulnerabilities (using the NPRM)
- Document both existing and potential countermeasures (using the NPRM)
- Prioritizing actions
- Develop and execute a plan

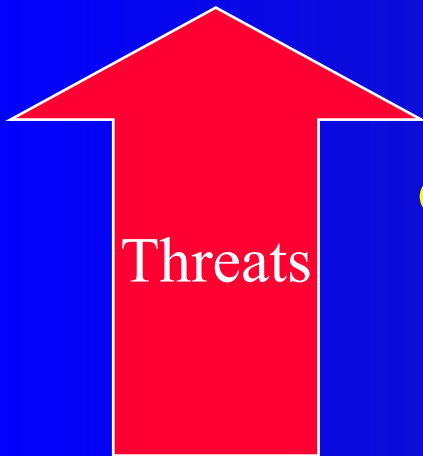
Potential Areas of Loss



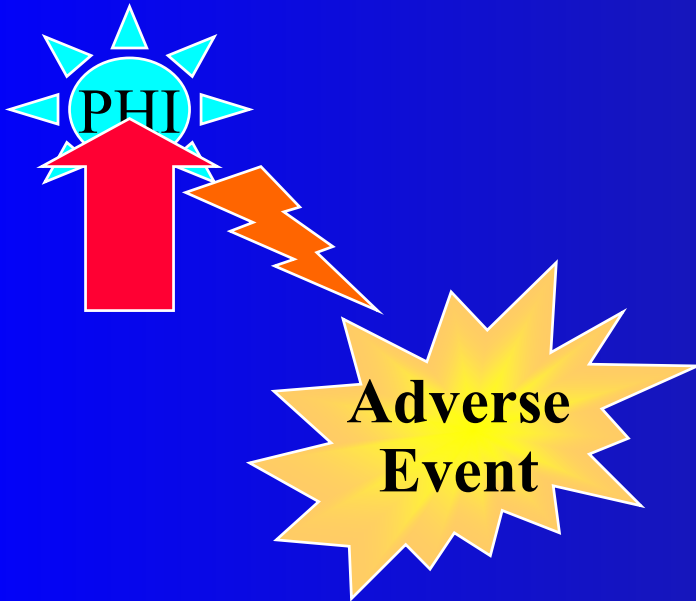
- Protected Health Information (PHI)
- Medical Equipment
- Intellectual Property
 - Processes and Procedures
- Physical Assets, including:
 - Information Systems
 - Telecommunications
- Public Confidence

Identify Threats

- Threats may trigger undesirable events
 - Do not require malicious intent
 - Can be random or specific
- Threats have three components
 - Targets (your valuable “stuff”)
 - Agents (someone or something)
 - Events (what can happen)



Potential Adverse Events



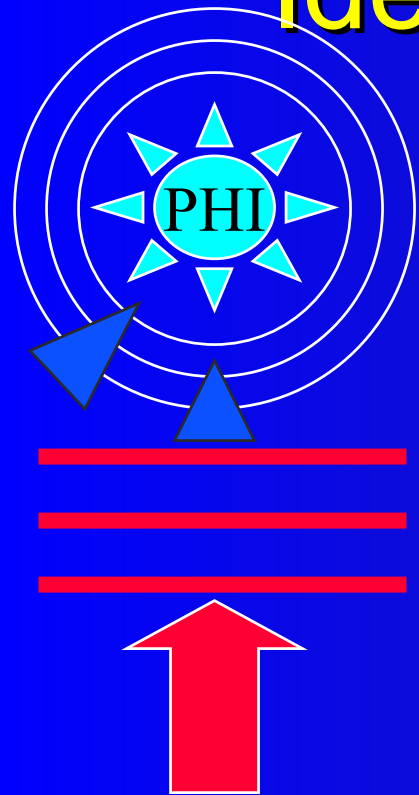
- Destruction
 - Accidental or malicious
- Alteration
 - Accidental or malicious
- Unavailability of data
- Theft or interception
- Unauthorized use
- Natural interruptions

Identifying Vulnerabilities



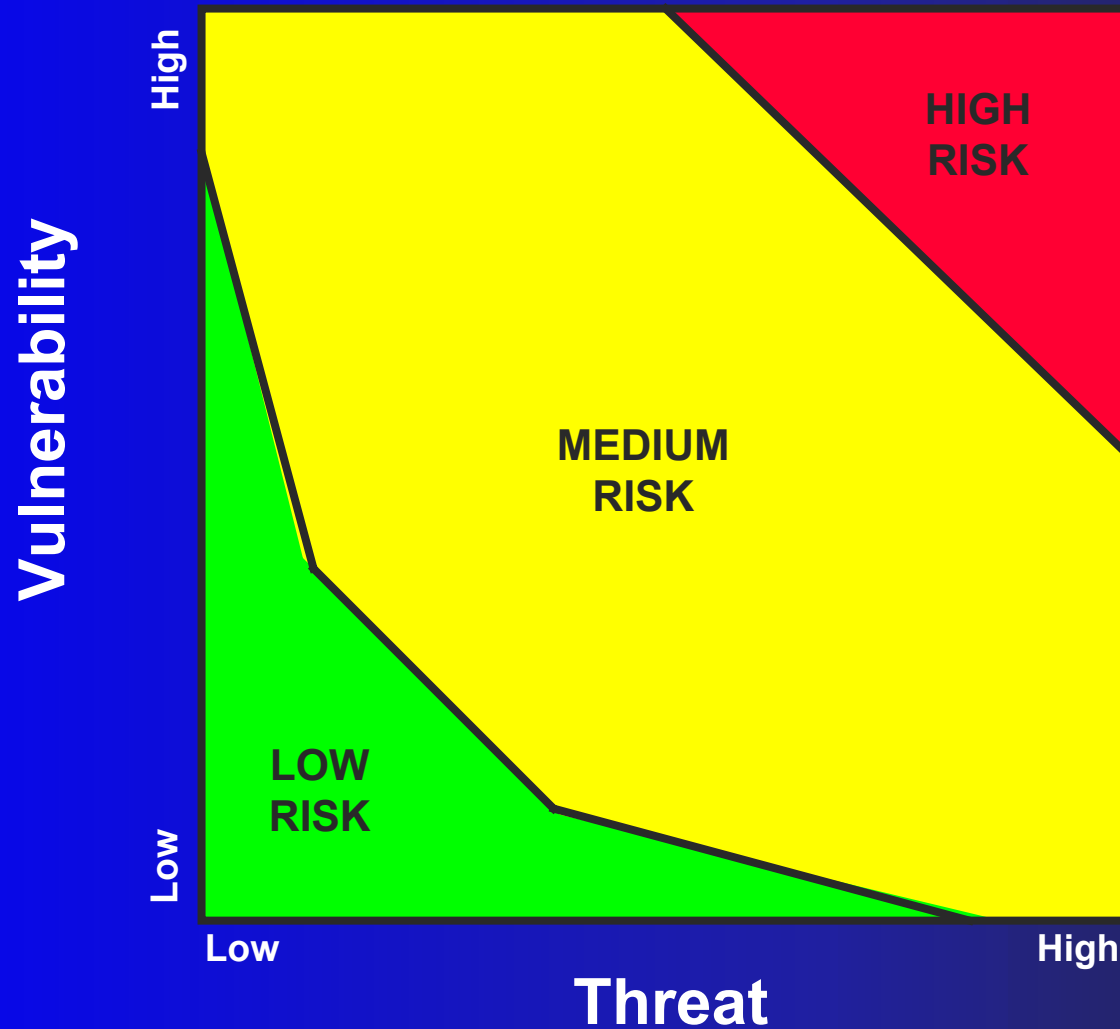
- Vulnerabilities are avenues of potential attack
- Vulnerabilities exist in:
 - Policies and procedures
 - Information Systems
 - Employees
 - Physical security
 - Business partners
- Security NPRM designed to counter vulnerabilities

Identify Countermeasures



- Countermeasures directly address vulnerabilities
 - Use your risk assessment methodology to identify both existing and potential countermeasures
 - Take advantage of “defense in depth”

Calculate Your Risk



NPRM Example #1

- **Threat:** Workstation location in lobby permits viewing by other patients
- **Potential Loss:** PHI information
- **Vulnerability:** No policy on workstation usage and placement
- **Risk:** HIGH
- New **Countermeasure:** Turn monitor so that it is not visible to other patients

Physical Security – Secure Workstation Location

NPRM Example #2

- **Threat:** Disgruntled employee may delete system data and disable backup tapes
- **Potential Loss:** PHI information
- **Vulnerability:** No policy about offsite storage and integrity of back-up tapes
- **Risk:** HIGH
- New **Countermeasure:** Periodically send copy of backup tapes to offsite location, ensure integrity through “restore” command

Security Configuration Control

NPRM Example #3

- **Threat:** New employees may inadvertently release restricted PHI
- **Potential Loss:** Public Confidence
- **Vulnerability:** Training policy does not require training prior to PHI access
- **Risk:** **MEDIUM**
- New **Countermeasure:** Modify employee training plans to require HIPAA Training signoff prior to authorizing access to PHI

Getting Started

- Form a HIPAA Security Team
 - Chief Security Officer
 - Technical support (IT and Physical)
 - Business management
 - Human resources
 - Policies and procedures
 - Training staff

Your Security Team's Goals

- Document the current security posture
- Document risks (threats X vulnerabilities)
- Make risk-based recommendations
- Implement approved recommendations
- Make security an integral part of your workforces' daily routine

Security Standard Summary

- Look at all aspects of the Standard together as a whole--the rules are interoperable
- Integrate the Privacy Standard in terms of:
 - Assessment for risk and vulnerability
 - Assessment for compliance
 - Development of Security/Privacy Policies & Procedures
- Lastly, this is not just a technology issue--far from it; this affects business and clinical policies and procedures, personnel, business partners, etc.
⇒ *As such, HIPAA doesn't belong to the CIO by default*

Final Rule - Privacy

- Covers electronic, paper & oral information
- Applies to Providers, Health Plans & Clearinghouses
- Requires contracts with business associates to protect health information
- Patient consent required for treatment, payment, & certain operations (QA, utilization review, credentialing)
- Limited sharing for “national priority” activities

Patients Rights

- Right to Timely Access to Records
- Right To Amend and Correct Records
- Right to review denials to amend or correct records
- Right To Restrict Use
- Right to Accounting of Disclosures
- Right to Revoke Authorization
- Rights of Deceased Persons

Final Rule - Privacy

- New consumer rights:
 - Requires written “fair information practices” that informs consumers as to how their information will be used and to whom it is disclosed.
 - Right of access to their record and for a copy
 - Right to request amendment of record in case of dispute
 - Right to request a record of disclosures for other than treatment, payment and operations

Final Rule - Privacy

- Boundaries on Record Use and Release
 - Release for other than treatment should be only the minimum necessary for the purpose (e.g., claims)
 - Restrictions on employer access to and use of employee's health information
 - Conditions on use of health information for marketing and solicitation purposes

Implementation Requirements

- Designate a privacy officer;
- Provide privacy training to workforce;
- Implement safeguards to protect health information from intentional or accidental misuse;
- Provide individuals with a means to lodge complaints about the entity's information practices, and maintain a record of any complaints.

Implementation Requirements

(cont)

- Develop a system of sanctions for members of the workforce and business partners who violate the entity's policies.
- Establish contracts with business associates that ensure that they exercise an appropriate level of care related to privacy.

Implementation Requirements

(cont)

- Policies and practices must be documented.
- Must have administrative systems, appropriate to the nature and scope of their business, that enable them to protect health information in accordance with the regs.

Implementation Issues

- **Scalability** - still to be decided, but more sophisticated entities may be expected to have more robust programs.
- **Reasonable** - within the range of latitude offered by the regs, you are only required to do what is reasonable, but the courts may be the deciding factor on what is reasonable.

Implementation Issues (cont)

- **Minimum Necessary Disclosure** for the task other than care of the individual between providers - be thoughtful about how much info needs to be revealed (inside and outside of the entity).
- **Preemption** – HIPAA is a floor; more stringent state laws/regs take precedence.
- **De-identifying** – remove identification info when feasible.

Penalties for Non-Compliance

- Violate transaction or security standards
 - Not more than \$100 per violation, maximum of \$25,000/year
 - No aggregate maximum
- Wrongful disclosures (privacy)
 - Not more than \$50,000 per violation
 - Imprisonment for not more than one year

Penalties for Non-Compliance (cont)

- False Pretenses (privacy)
 - Not more than \$100,000 per violation
 - Imprisonment not more than five years
- Intent to sell, transfer, or use (privacy)
 - Not more than \$250,000 per violation
 - Imprisonment for not more than ten years

5-step Process for Studying the Privacy Regulation

<http://aspe.hhs.gov/admnsimp/>

- Read HHS Press Release (3-pp)
- Read HHS Fact Sheet (5-pp)
- Read Regulation (31-pp)
- Read Guidance (53-pp)
- Read Preamble and Comments (338-pp)

COMPLIANCE STRATEGIES

Steps to Compliance

- Awareness & Education
- Form HIPAA Team
- Self-evaluation / Gap Analysis
- Risk Analysis
- Compliance Plan, Budget & Timeline
- Execute Plan
- Reevaluate Plan and Adjust with New Regulations

What can you do to get ready ?

- Intensify personal understanding of HIPAA
- Cooperate with other practices or peers in developing standard of care and best practices that are “reasonable”
- Adopt consensus best practices to avoid being outside the norm
- There is safety in numbers !

Resources

- DHHS/HIPAA: aspe.hhs.gov/admnsimp
- NCHICA: www.nchica.org
- WEDi/SNIP Web site: snip.wedi.org
- Transactions and Code Sets including implementation guides: www.wpc-edi.com/hipaa
- ASC X12N Standards: www.wpc-edi.com/hipaa



Self-assessment / Gap Analysis Tools

HIPAA EarlyView™ Security

HIPAA EarlyView™ Privacy

Questions ???

NCHICA

**North Carolina Healthcare
Information & Communications
Alliance, Inc.**

www.nchica.org

P.O. Box 13048

Research Triangle Park, NC 27709-3048

Voice: 919.558.9258 or 800.241.4486

Fax: 919.248.2198

nchica@nchica.org