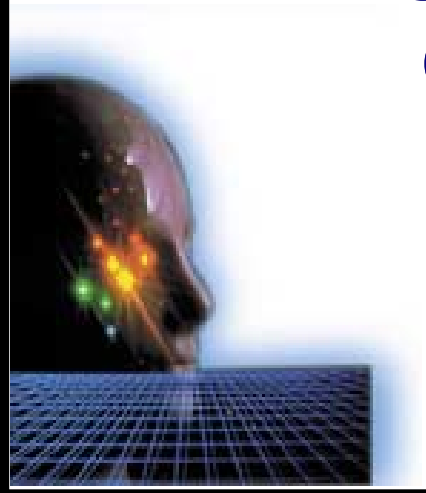
HIPAA Services

# HIPAA

## Health Insurance Portability & Accountability Act

## Administrative Simplification

## Understanding the HIPAA Choices and Challenges



# *Presentation Overview*

- **HIPAA Background and Purpose**
- **Security and Privacy**
- **Transactions, Code Sets and National Health Identifiers**
- **Getting Started**

# *HIPAA Background and Purpose*

# *HIPAA is one of the most far reaching pieces of healthcare legislation ever enacted...*

- **The Health Insurance Portability and Accountability Act of 1996 (HIPAA) sets forth specific provisions for:**
  - Standardized health information transactions
  - Standardization of code sets (e.g., CPT, ICD, etc.)
  - National identifiers for providers, health plans/payers and employers
  - Security and privacy of health information
- **HIPAA regulations represent both *risks* and *opportunities* for healthcare payers and providers:**
  - Opportunity to leverage the intended simplification of HIPAA for administrative cost savings and implementation of eCommerce solutions
  - Responsibility to comply with requirements that protect the privacy of personal health information - a topic of increasing concern to consumers and regulators

# *. . . and will affect ….*

- Health Plans, Healthcare Clearinghouses and Healthcare Providers
- The goals of the Administrative Simplification are to:
  - Improve the efficiency and effectiveness of the health care system
  - Standardize the electronic data interchange of certain administrative financial transactions
  - Protect the security and privacy of transmitted information

# HIPAA

**Final Rule on Transactions and Code Sets published August 17, 2000, for implementation October 16, 2003. Final Rule on Privacy published December 28, 2000 for implementation April 14, 2003.**

## Title I Portability

## Title II Administrative Simplification

### Transaction Standards

#### Data Element

- Required vs. Optional
- Format
- Non-Medical Codes
- Values

#### Transaction Sets

- ASC X12N version 4010 mandated
  - Claims - 837
  - Eligibility - 270/271
  - Referral Certification and Authorization - 278
  - Claim Status - 276/277
  - Benefit Enrollment and Maintenance - 834
  - Claim Payment and Remittance Advice - 835
  - Premium Payments - 820
  - Additional Information to Support Claims/Encounters **(not yet final)** - 275
  - First Report of Injury **(not yet final)** - 148
- NCPDP 5.1 mandated for pharmacy transactions (claims, eligibility, and payment/remittance)

### Standard Code Sets

#### Medical Codes

- ICD-9-CM
- CPT-4
- HCPCS
- CDT
- NDC (probable revision)
- No local codes
- No "J" codes (probable revision)

### Unique Health Identifiers

#### Provider

- Single NPI: 10 position numeric, one digit checksum (no location code)
- No embedded intelligence

#### Employer

- 9 position numeric, one digit checksum
- Tax ID Number
- No embedded intelligence

#### Health Plan (no NPRM issued)

- 10+3 position numeric, one digit checksum
- Sub-ID may appear on health card & direct EDI
- No embedded intelligence

#### Individual

- Unlikely to be finalized

### Security

#### Administrative Procedures

- Chain of Trust Agreement
- Designated Security Officer
- Certification, Internal Audit, Training, Policies, BCP, etc.

#### Physical Safeguards

- Secure Workstations
- Physical Access Controls for Network/Computer H/W, etc.
- Facilities, Media Disposal, etc.

#### Technical Security Services

- Access Controls
- Authorization
- Data Authentication
- Entity Authentication

#### Technical Security Mechanisms

- Basic Network Safeguards
- Integrity and Protection

#### Electronic Signature

- Not required for any current HIPAA-mandated transactions

### Privacy

#### Applicability

- Covers protected health information (PHI) stored or transmitted in any form or medium: electronic, paper and oral

#### Key Elements

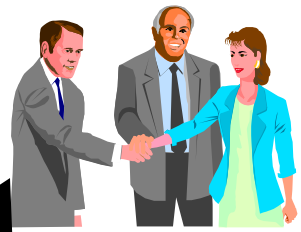
- PHI data elements defined
- Notice of privacy practices mandated
- Minimum necessary disclosure/use
- Consent required for routine use
- Authorization required for non-routine use
- Business associate contracts required
- Designated Privacy Official

***HIPAA Provisions as of December 2001***

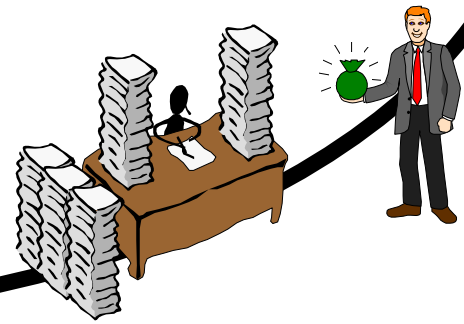
# *HIPAA impacts Physicians, Care Providers, Health Information Managers, Revenue Cycle Personnel, Patients, Health Plans*

***Physician Impact: Patient Care, Documentation, and Confidentiality***

***Operations Impact: Health Information, Medical Records, Member, Patient and Physician Relations***

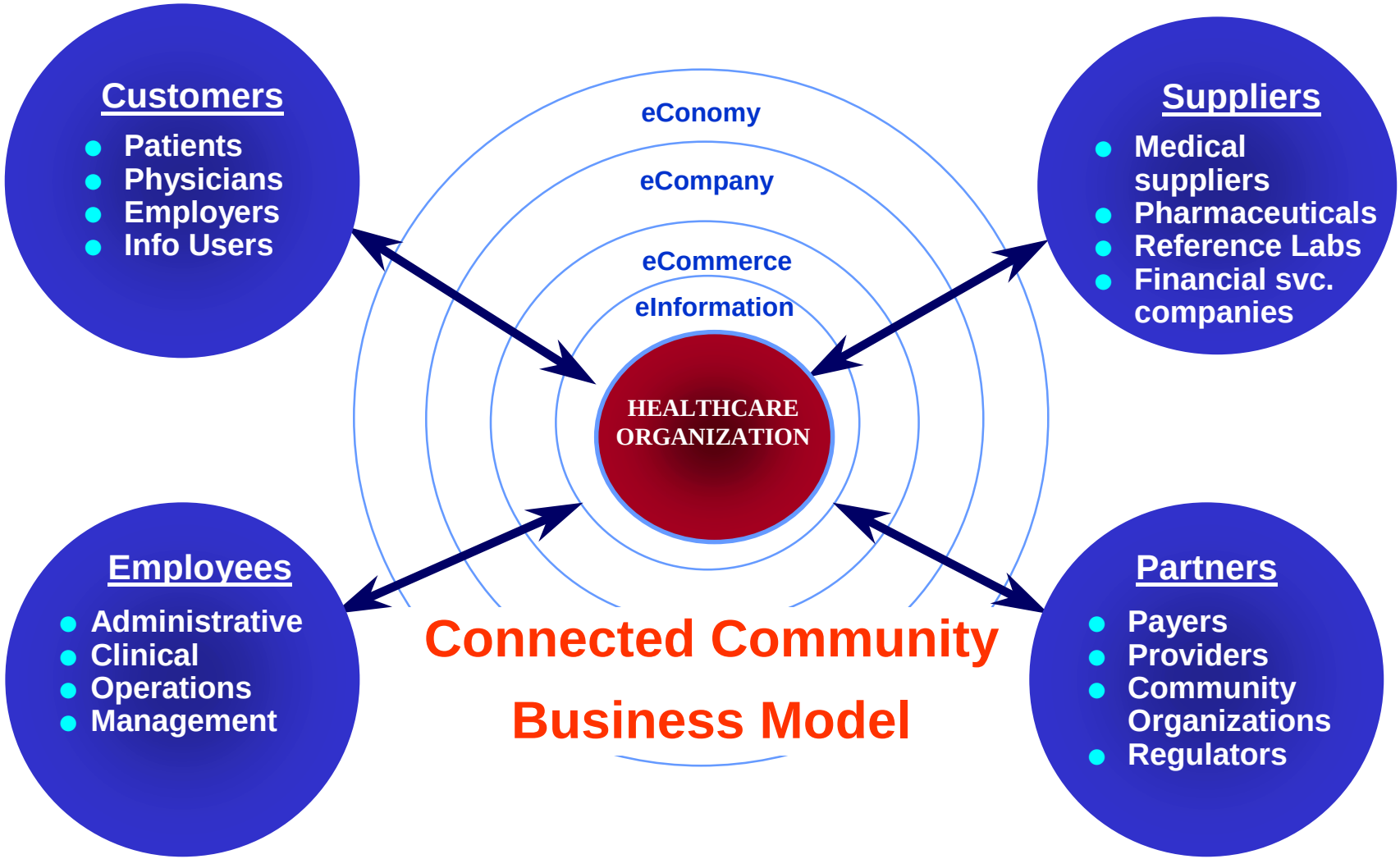


***Patient Impact: Increased focus on privacy, health information management, enhanced physician-hospital communication***



***Revenue Cycle Impact: Patient Accounts, Provider-Payer Communication, Administrative Simplification***

# *HIPAA enables healthcare organizations to capitalize on, not just conform to, e-Business opportunities with key constituents ...*



# *HIPAA is inextricably linked to an organization's strategic business initiatives…*

**The HIPAA requirements are inextricably linked to those business objectives which will help organizations achieve a strategic advantage within this new connected community business model:**

- **Enables entities to fully utilize the internet for e-Commerce including transmission of claims and other connectivity with business partners and users;**
- **Federally mandated new standards for Electronic Data Interchange (EDI) to support paperless patient account environments, improve cash flow, and reduce cost of billing and collections;**
- **Electronic Medical Record to provide enterprise-wide access to critical health information; and,**
- **Enterprise Decision Support Information**

***An organization simply will not be able to discuss these objectives without considering the compliance or enabling implications of the HIPAA requirements.***

# *Implications of HIPAA are significant across the health industry…*

- **Assessment and implementation will take time, planning, resources, and change - this is *not* an overnight fix**
- **Security and privacy are primary consumer concerns - not addressing them proactively will result in the loss of trust, credibility, and potentially revenue**
- **Penalties and fines are modest for non-compliance with transactions; civil and criminal penalties for non-compliance with security and privacy are more severe.**
- **However, major impact is on ability to do business**

***"Without safeguards to assure that obtaining health care will not endanger our privacy, public distrust could turn the clock back on progress in our entire health care system."***

**- Former Secretary Shalala, Department of Health & Human Services**

# *Privacy and Security*

# *There are a multitude of privacy and security violations*

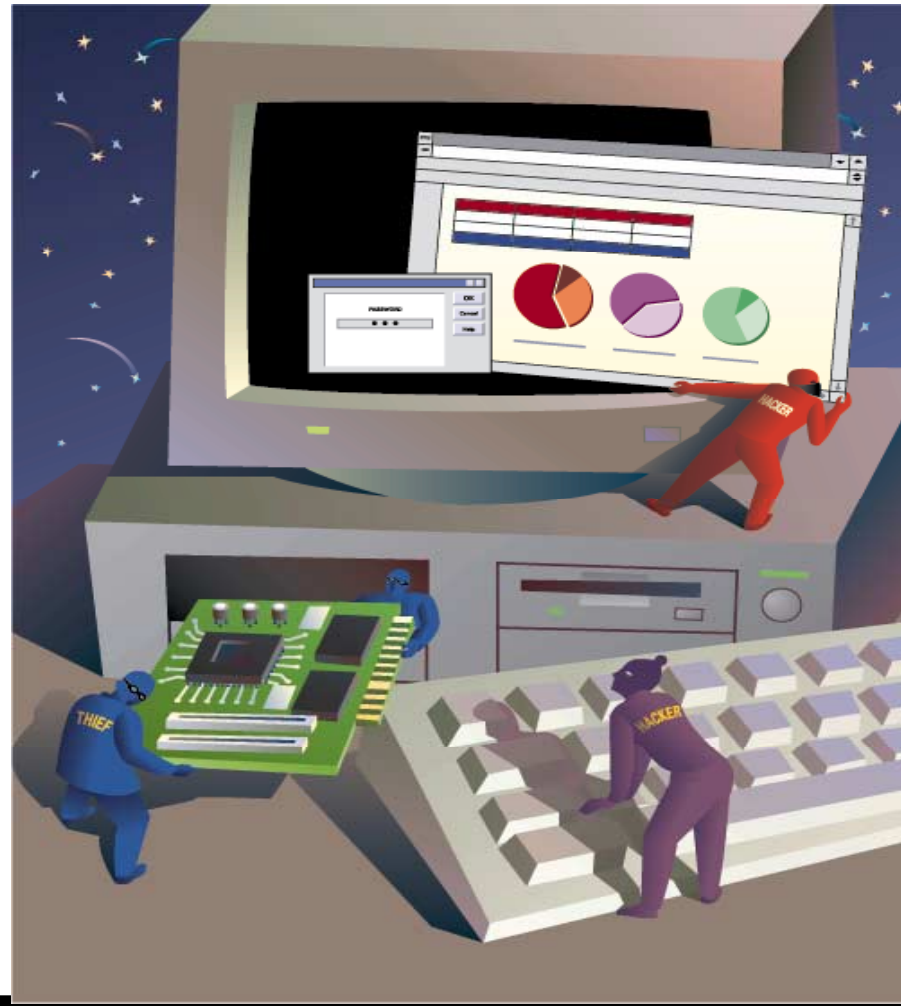
- **A Michigan health care system accidentally posted medical records of thousands of patients on the Internet.**
- **An employee of the Tampa health department took a computer disk containing names of 4000 HIV positive patients. The disks went to two newspapers.**
- **HCFA 1500 billing forms "blew out" of a truck going down I-95 in Connecticut.**
- **Two health care organizations in Washington state were found discarding medical reports in unlocked dumpsters.**
- **More listed on the Health Privacy Project website (Institute for Health Care Research and Policy from Georgetown University) at www.healthprivacy.org.**

# *Privacy - Benefits*

- Mitigate business risks and legal liability around privacy issues
- Builds the ethical corporate culture based on respect for individual privacy
- Meet emerging governmental standards
- Increase consumer and brand loyalty
- Build consumer trust and confidence - allows for greater use of connectivity and eCommerce

# *HIPAA Privacy Regulations*

- Final rules were published 12/28/00 and became effective 04/14/01
- Implementation date of 04/14/03 (4/14/04 for Small Health Plans)
- Applies to: Any entity collecting, creating, maintaining or disseminating individually identifiable health information (IIHI)



# Privacy - Overview

- The burden of ensuring privacy of protected health information (PHI) will disproportionately lie with the providers and will be among the most far-reaching of the HIPAA requirements to implement.
- It is important for an organization to consider the potential impact of changes implemented to comply with the privacy (and security) requirements, and to consider other important organization values and objectives when designing solution alternatives, such as:
  - Support the necessary flow of patient information to physicians and other caregivers for the purposes of continuity of care;
  - Support the needs of legitimate research and quality management initiatives;
  - Manage accounts receivable;
  - Manage the cost of clinical and support operations
  - Maintain fair and collegial relationships with business associates

**It is important to engage internal or external legal counsel and risk management or compliance departments in the planning process for purposes of legal interpretation and insuring that policies or practices recommended are consistent with the organization's overall ideals.**

# *HIPAA Privacy Regulations - E&Y's Point of View*

- HIPAA privacy requirements need not inhibit legitimate access to information.
- Compliance requires a thoughtful examination of access to and the use of protected health information (PHI) on an enterprise-wide basis.
- Privacy is not a technical issue; it's an organizational performance and cultural issue which will require supporting technology and business processes.
- Early compliance with HIPAA privacy regulations will create opportunities for competitive advantage.
- Specific requirements to demonstrate due diligence in complying with HIPAA privacy regulations is likely to remain somewhat ambiguous. Acceptable best practices will emerge in the market over time.
- A written privacy policy is a key starting point for compliance with HIPAA privacy regulations. It represents both:
  - An external communication of the organization's commitment to the privacy of PHI, including a clarification of permitted uses in the normal course of operations.
  - An internal statement of the organization's values and policies regarding the secure treatment of PHI, including expectations of employees and associates, and the consequences of failure to meet those expectations.

# Individually Identifiable Health Information

- *any **information**, including demographic information **collected from an individual**, that*
  - *is **created or received** by a health care provider, health plan, employer or health care clearinghouse, and*
  - *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 **identifies the individual or** with respect to which there is a reasonable basis to believe **that the information can be used to identify the individual.***

# PHI – Individually Identifiable Data Elements

- Name
- Address (Street Address, City, County, Zip Code or Other Geographic Codes)
- Names of Relatives
- Names of Employers
- Birth Date
- Telephone Number
- Fax Number
- Email Addresses
- Social Security Number
- Medical Record Number
- Health Plan Beneficiary Number
- Account Number
- Certificate/License Number
- Vehicle or Device Serial Number
- Web URL
- Internet Protocol (IP) Address
- Finger or Voice Prints
- Photographic Images
- Any other unique identifying number, characteristic, or code (whether generally available in the public realm or not)

# Five Key Areas of Privacy Standards

| Boundaries | Security | Consumer Control | Accountability | Public Responsibility |
|---|---|---|---|---|
| ▲ Information used only for intended purpose<br>▲ Consumer disclosure statement | ▲ Administrative, technical, and physical mechanisms to keep information private, confidential and secure within internal operating systems and external communications | ▲ Informed consent to use information<br>▲ Right to access and amend information<br>▲ Record of disclosures | ▲ Federal penalties for violations<br>▲ Effective compliance activities to deter, identify, and punish violations | ▲ Process for disclosing information for public health, research & legal purposes |

## Frequently Asked Questions (FAQs)

1. **What is the Protected Health Information covered in HIPAA?** PHI is individually identifiable health information electronically maintained or transmitted, or in any other media or form. Identifiable information includes: name, address, employer, relatives' names, DOB, telephone and fax numbers, e-mail addresses, IP addresses, SSN, medical record number, member or account number, certificate/license number, voice/fingerprints, photos, or other number, code or characteristics (e.g., occupation).
2. **What kind of official oversight will organizations need?** Each organization will be required to have a Privacy Official.
3. **Where can I go to learn more about the privacy standards?** You may visit the Ernst & Young HIPAA web page... http://www.ey.com/us/hipaa.

# Examples of Operational Impact Relating to Privacy

- Patient Rights
  - Patients must be informed of their rights
  - Patients will have the right to inspect and amend their information
  - Defined process for handling patient complaints
- Patient Access
  - Opportunity to reduce costs and increase customer satisfaction regarding eligibility, verification, and referral authorization
  - Caregivers will generally have burden of responsibility for securing the "general consent" and providing the notice of privacy practices
- Health Information Management (Medical Records)
  - New rules for disclosing patient information
  - New mechanisms for accounting for certain types of disclosures
  - Will affect all areas responsible for managing medical records and/or disclosures of patient information
  - Audit trails to monitor access/modifications to patient information

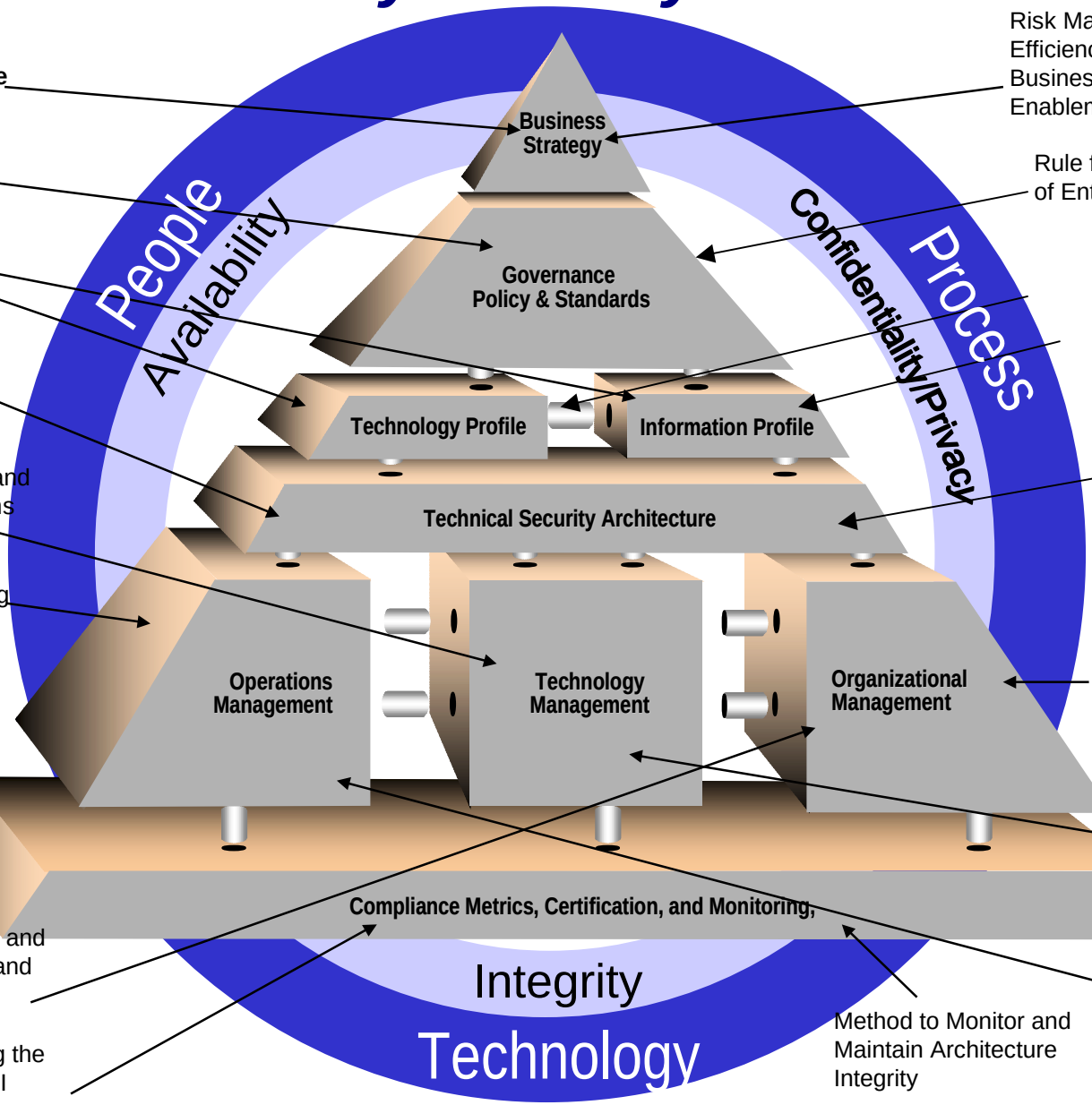
# Security - Overview

- Sound security policies and practices provide a foundation for safeguarding PHI.
- Although technology attributes of a security are important, the business processes and workforce behaviors are an even more critical component.
- Since they are based on industry models, the proposed security requirements are expected to be relatively unchanged when the final regulations are published.
- Compared to the privacy requirements, performing a security assessment would be a fairly well-defined process.

| Administrative Procedures | Physical Safeguards | Technical Standards & Mechanisms |
|---|---|---|
| ▲ Certification review<br>▲ Chain of trust agreements<br>▲ Policies & procedures<br>▲ Access Authorization<br>▲ Proactive internal audit<br>▲ Personal authorization<br>▲ Security mgt. process<br>▲ Termination process<br>▲ Training | ▲ Assigned responsibility<br>▲ Media controls over hardware & software<br>▲ Access controls<br>▲ Workstation policies<br>▲ Secure workstations<br>▲ Training | ▲ Access controls<br>▲ Audit controls<br>▲ Authorization control - use & disclosure<br>▲ Data authentication<br>▲ Entity authentication |

# HIPAA Privacy/Security Architecture

HIPAA Services




**HIPAA, NAIC, HEDIS, CMS, and JCAHO Compliance**

Risk Management, Efficiency Enhancement, Business Process Enablement

Rules for Using and Protecting IIHI

Rule for Protection and Use of Enterprise Information

Identification of IIHI and Where It Resides

Identification of Sensitive Business Information such as Legal, Financial, Strategic, HR, Etc. and Where it Resides

Network and System Architecture and other Tools to Protect IIHI

Security Impact of Enterprise Network and System Architecture - Vulnerabilities on non-PHI Systems may Expose PHI

Security configuration and management of systems hosting IIHI

Practices for Supporting Operations (Tape Backup, Application Execution, Etc.) on Systems Hosting IIHI

People Element of Information and Systems Management

Technology Element of Information and Systems Management

Roles, Responsibilities, and Practices for Handling and Using IIHI

Process Element of Information and Systems Management

Practices for Monitoring the Security and Use of IIHI

Method to Monitor and Maintain Architecture Integrity

# Examples of Operational Impact Relating to Security

- Focus on Documentation
  - Documented security policies
  - Policies for monitoring effectiveness
  - Metrics to measure need for improvement
  - Reporting, auditing and acting upon the metrics
- Heavy Emphasis on Training and Awareness
  - Initial and ongoing education
  - Self assessments and risk assessments
  - Measuring performance
  - Documented steps when improvement required
- Mental Change
  - Automatic workstation logoffs, stringent password requirements, no password sharing
  - Possible inefficiencies

***Technology is where organizations have been focusing – technology enablement is not relevant without change in processes and culture.***

# *Transactions, Code Sets and National Health Identifiers*

# Transactions, Code Sets and National Health Identifiers - Overview

- Substantive “meat” of the activity within the Department of Health and Human Services for rule making since the legislation was passed.
- Constitutes the means for Administrative Simplification and Portability.
- Will affect both Payers and Providers to a differing degree.
- Payers, clearinghouses and software vendors will clearly have the majority of the burden to remediate their information systems.
- Providers should be aware of the “state of readiness” of these third parties and be prepared for changes they must make to their infrastructure.
- Also, to the extent they may develop and maintain custom applications, Providers will have a responsibility to remediate their own applications, or customization to vendor-supplied applications.
- Organizations should also anticipate impacts on key business processes.

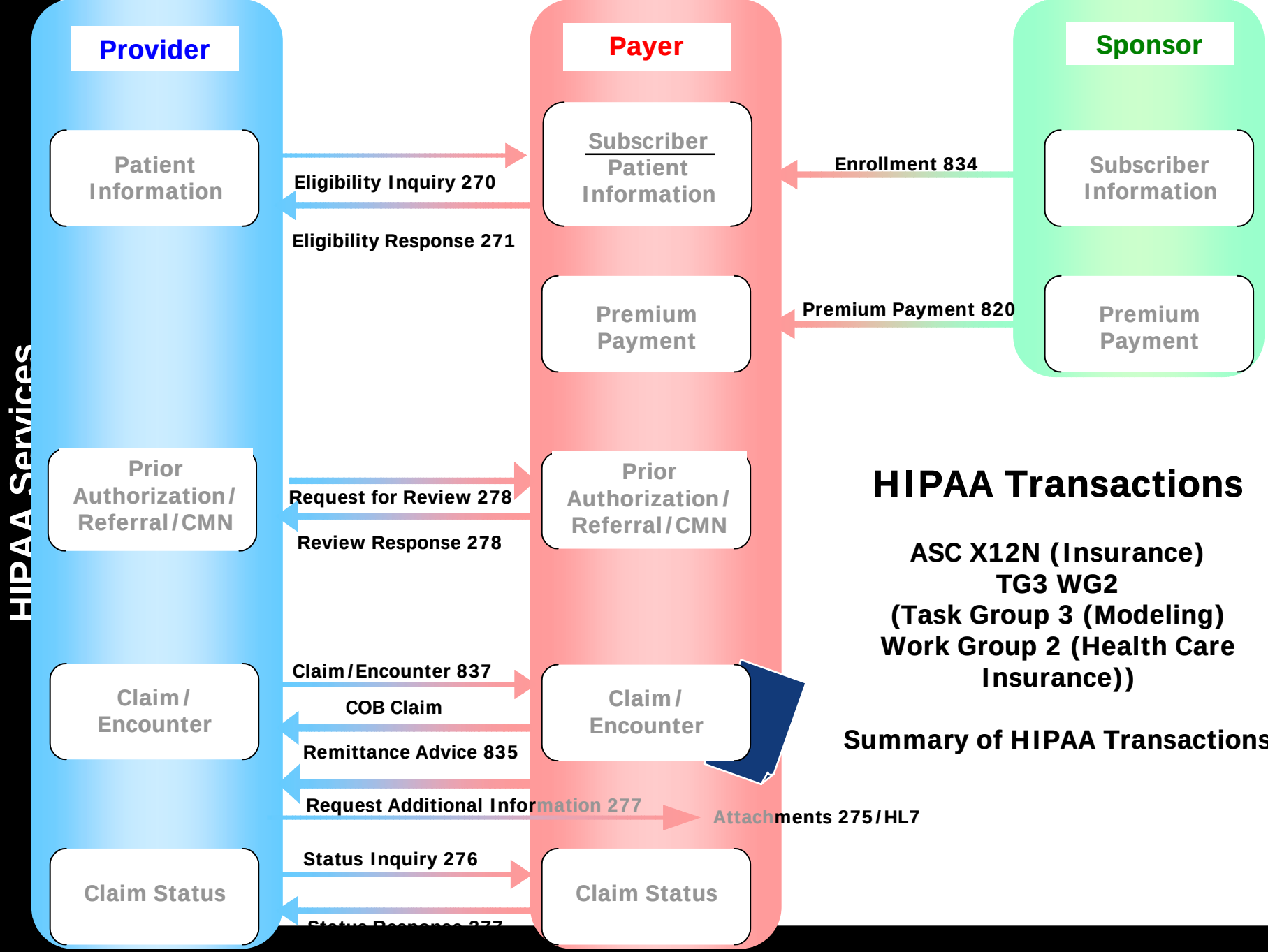
# The transaction standards include:

| 270/271<br>Inquiry/Response for Eligibility | 275<br>Request for Additional Support for Claim | 276/277<br>Inquiry/Response for Claims Status | 277<br>Unsolicited Request for Additional Info | 278<br>Authorizations and Referrals |
|---|---|---|---|---|
| Inquiry/ response for verification of an individual's eligibility, benefits and coverage. | Request for additional information to support a health care claim and/ or encounter.<br>This transaction has finalized the HL7 embedded portion of the standard but has not finalized the ANSI portion.<br>NOTE: This transaction is scheduled to be finalized at a later date. | Request/response for health claim status. | Health care claim request for additional information needed to complete adjudication process. | Receive and respond to requests for authorization or certification from providers. |

| 820<br>Premium Payment/Order Remittance Advice | 834<br>Benefit and Enrollment Maintenance | 835<br>Health Care Payment/ Advice | 837<br>Health Care Claim | First Report of Injury |
|---|---|---|---|---|
| Receive payroll deductions & other group premium payments from employers for insurance products.<br>Additionally there is an 811 transaction (Consolidated Billing) that is complementary to the 820 transaction, but is not required as part of HIPAA. | Receive enrollment information for insurance coverage benefits or policy from other sponsors of insurance coverage. | Payment of health care claims and transfer of admittance advice (EOB) to providers. | Receive health care claims and encounters from providers. | This transaction set has not yet been finalized. |

## Frequently Asked Questions (FAQs)

1. **Can health care providers/payers selectively implement transaction statements?** No, all transactions will be covered including: health claims, enrollment & disenrollment, eligibility, payment and remittance advice, premium payments, claim status, referral, certification & authorization and COB. Standards for first report of injury will be proposed at a later date.


HIPAA Services
Provider
Payer
Sponsor
Patient Information
Subscriber Patient Information
Subscriber Information
Eligibility Inquiry 270
Eligibility Response 271
Enrollment 834
Premium Payment
Premium Payment
Premium Payment 820
Prior Authorization / Referral / CMN
Prior Authorization / Referral / CMN
Request for Review 278
Review Response 278
Claim / Encounter
Claim / Encounter
Claim/Encounter 837
COB Claim
Remittance Advice 835
Request Additional Information 277
Attachments 275/HL7
Claim Status
Claim Status
Status Inquiry 276
HIPAA Transactions
ASC X12N (Insurance)
TG3 WG2
(Task Group 3 (Modeling)
Work Group 2 (Health Care Insurance))
Summary of HIPAA Transactions

# First Set of Transactions

- Based on existing X12N (version 40.10), NCPDP and ADA transactions.
- The X12N standard for claims includes standard information for coordination of benefits.
- Final rules on transactions were published 8/17/00 and became effective 10/16/00.
- HR 3323 was signed into law on 12/27/2001 allowing for a one-year extension if a compliance plan is submitted to DHHS by 10/15/2002.
- Implementation required by 10/16/2002 if no compliance plan is submitted and 10/16/2003 if a compliance plan is submitted (small health plans are to be compliant by 10/16/2003)
- Changes in the standards can occur as often as once a year with 6 months notice.

# H.R. 3323 Requirements

- Compliance plan that includes:
  - An analysis of current non-compliance (scope and reasons why)
  - A budget, schedule, work plan and implementation strategy for achieving compliance
  - Whether a contractor or other vendor might be used to achieve compliance
  - A timeframe for testing to begin no later than April 16, 2003
- Model compliance form to be developed by DHHS by March 31, 2002 with electronic submission of the compliance plans permitted
- Providers stop submitting paper claims to Medicare – only electronic claims submission will be allowed (some exceptions apply for small providers or those without electronic access methods)

# *Do not under estimate the effort to achieve transactions, code sets, identifiers compliance…*

| *Compliance Remediation Activity* | *Responsibility* | |
|---|---|---|
| | **Package Vendor** | **Provider** |
| Base Software | ⚑ | |
| Testing Base Software Remediation | | ⚑ |
| Operational processes, policies, procedures | | ⚑ |
| Software adaptations using vendor tools | | ⚑ |
| Custom queries | | ⚑ |
| Report writing subsystems | | ⚑ |
| Inhouse converter/translation tables, databases, repositories, warehouses | | ⚑ |
| Interfaces | | ⚑ |

# *Code sets are unique coding standards used to identify diagnostic procedures, diagnosis and medical supplies on health care claims and billing forms.*

| ICD-9-CM | HCPCS | CPT 4 | NDC | CDT |
|---|---|---|---|---|
| International classification of diseases and diagnosis. This code is used to identify an individual's disease and/ or diagnosis on a health care claim or encounter.<br><br>There are three levels of ICD-9 codes:<br>▲ Level I - Diagnoses<br>▲ Level II - Diagnoses<br>▲ Level III - Procedures | Standard codes used by Medicare to identify procedures performed by a provider on an individual an a health care claim and encounter. | Standard procedure code used by the health care industry to identify the procedure performed on the individual by the provider on a health care claim and encounter. | National standard drug codes used to identify drugs on a health care claim or encounter. | National standard dental codes and terminology used to identify dental diagnosis on dental claims. |

## Frequently Asked Questions (FAQs)

1. **Can local codes continue to be used?** All local codes will be eliminated once the new standard codes are implemented.

2. **Will health organizations be able to apply for exceptions?** Organizations will be able to apply to Health and Human Services (HHS) for exceptions in unusual cases where codes are required but do not currently exist.

3. **Will the implementation of new code set standards eliminate state specific codes?** The new code sets are not intended to eliminate state specific codes but will eliminate redundant codes. States will have to apply for an HHS exception to continue to use state specific codes.

4. **When will ICD-10 and CPT-5 codes be implemented?** ICD-10 and CPT-5 code sets will not be implemented before 2003.

***Health Identifiers are assigned numbers and/or alpha numeric characters used to identify a provider, provider group or organization, health plan (payer) and employer needed to process all health encounter and claim information.***

| NPI (Provider) | EIN (Employer) | Plan ID (Health Plan) |
|---|---|---|
| Unique identification number for health care provider that will used by all health plans. Health care providers, all health plans and clearinghouses will use the NPIs in administrative and financial transactions specified by HIPAA. | Unique identification number used to identify employers and employer groups. EIN will be used to simplify administrative and financial transactions specified by HIPAA. | National standard plan identification number to be used by all health plans, employers and other health care participants to provide efficient electronic data interchange and health care administrative process. |

## Frequently Asked Questions (FAQs)

1. **What is the NPI?** The NPI is a unique identification number for health care providers. As of the most recent information available, the NPI will be a 10 digit numeric code randomly assigned to health providers.
2. **Does the NPI replace the Tax Identification Number?** The NPI will not replace the TIN but will eventually replace the UPIN.
3. **Will the NPI contain embedded logic or local designation codes?** The NPI will not contain any embedded logic. At this time, local designations are being considered but it is unlikely they will be included in the final ruling.
4. **What is the employer identifier?** The EIN will likely be the employer tax ID number.

# *Getting Started*

# *Developing an Enterprise HIPAA Strategy*

- The strategy should consider:
  - E-Commerce
  - Technology
  - Processes
  - Policies (incorporate as part of corporate compliance)
- Establish HIPAA Task Force with an enterprise-wide focus
- Perform Current State Assessment of readiness
- Develop and deliver HIPAA awareness program
- Establish budgeted resources and dollars
- Develop a plan for action, including prioritized remediation efforts, infrastructure changes, resource needs

# *A Total Solution*

- Gap Assessment
- Implementation Planning
- Implementation
- Business processes, policies, procedures
- Package and custom applications
- Organizational change management
- Learning solutions
- Program management
- Forming alliances with key vendors, especially those providing alternative solutions