HIPAA Administrative Simplification Provisions

AN OVERVIEW

Brent Saunders
Partner
PricewaterhouseCoopers
Florham Park, NJ
(973) 236-4682

p w c

Presentation Agenda

- HIPAA Background and Overview
- Proposed Security Regulations
- Final Technology Regulations
- Current Final Privacy Regulations
- Pharma – Potential Areas of Impact

Background of HIPAA

P w C

HIPAA General Provisions

- **Group and Individual Insurance Reform**
  - Limits on pre-existing exclusion provisions
  - Portability of coverage, guaranteed issue and renewal
- **Fraud and Abuse**
  - Medicare integrity, data collection, beneficiary incentive programs
  - Increased penalties, sanctions, and exclusions
- **Tax-Related Health Provisions**
  - MSAs, long-term care insurance, taxation of insurance benefits
- **Administrative Simplification (AS)**
  - Improve efficiency and effectiveness of the healthcare system
  - Define standards for electronic transmission - standard identifiers, transaction and code sets
  - Protect the privacy and security of health information

What is Administrative Simplification?

The Administrative Simplification provisions of HIPAA were enacted by Congress to regulate and standardize information exchanges and establish standards for the privacy and security of individually identifiable health information.

Four key areas of Administrative Simplification:

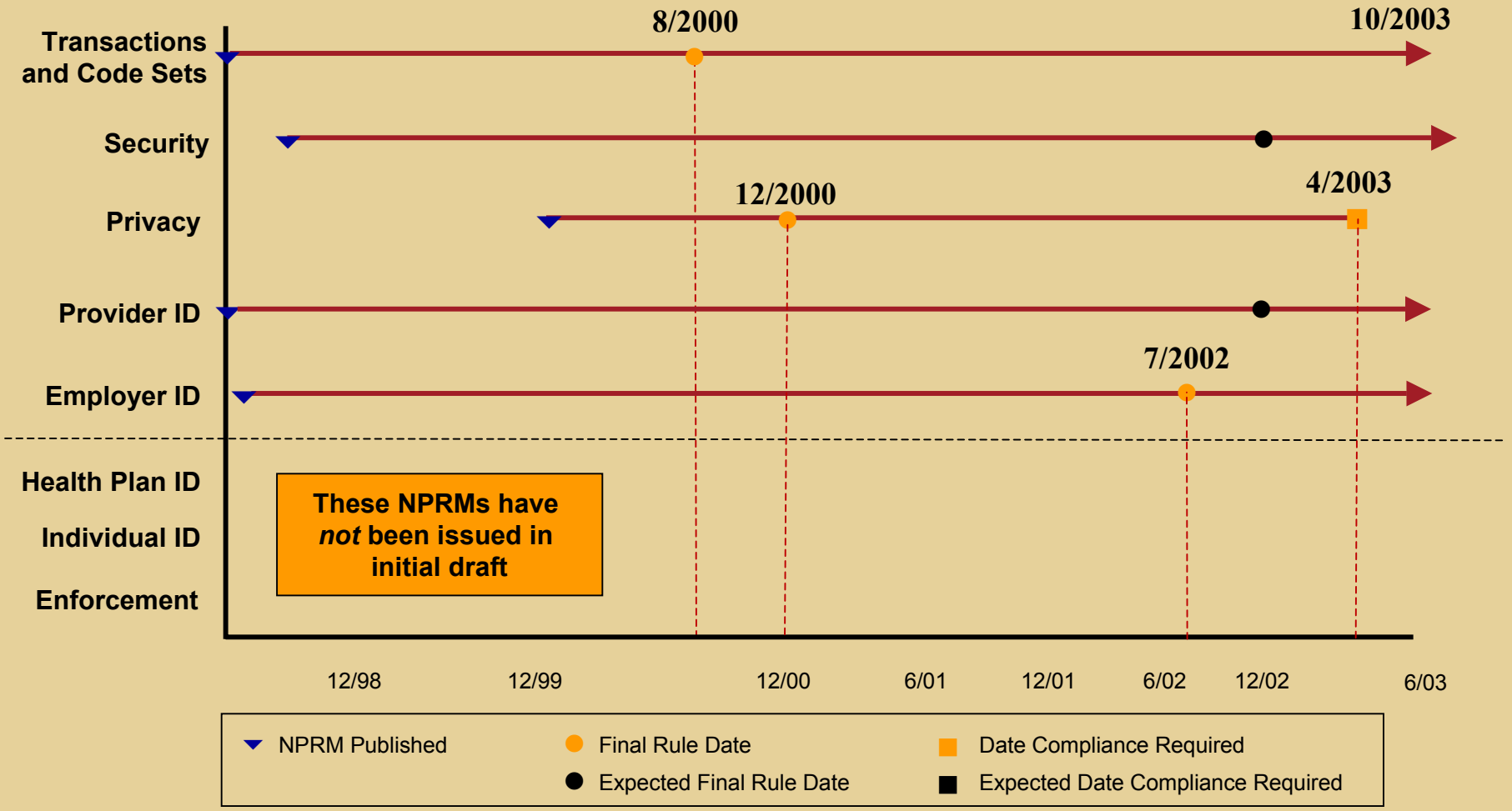
- Transactions and Code Sets
- Unique Identifiers
- Security
- Privacy

Applicability - Covered Entities

- Health plans
  - Health insurers
  - HMOs
  - ERISA plans
  - Medicare+Choice
  - Long Term Care Insurer
  - Indian Health Service
  - Veteran's Administration
  - Active military
  - CHAMPUS
  - Medicaid and Medicare
  - Medicare supplements
  - FEHBP, CHIPS
- Providers*
  - Physicians
  - Hospitals
  - Laboratories
  - Pharmacies/PBM
  - Ambulatory care centers
  - Dentists
  - DME suppliers
  - Home care agencies
- Healthcare clearinghouses
  - Receive non-standard data or transactions from covered entities for conversion into standard data or transactions

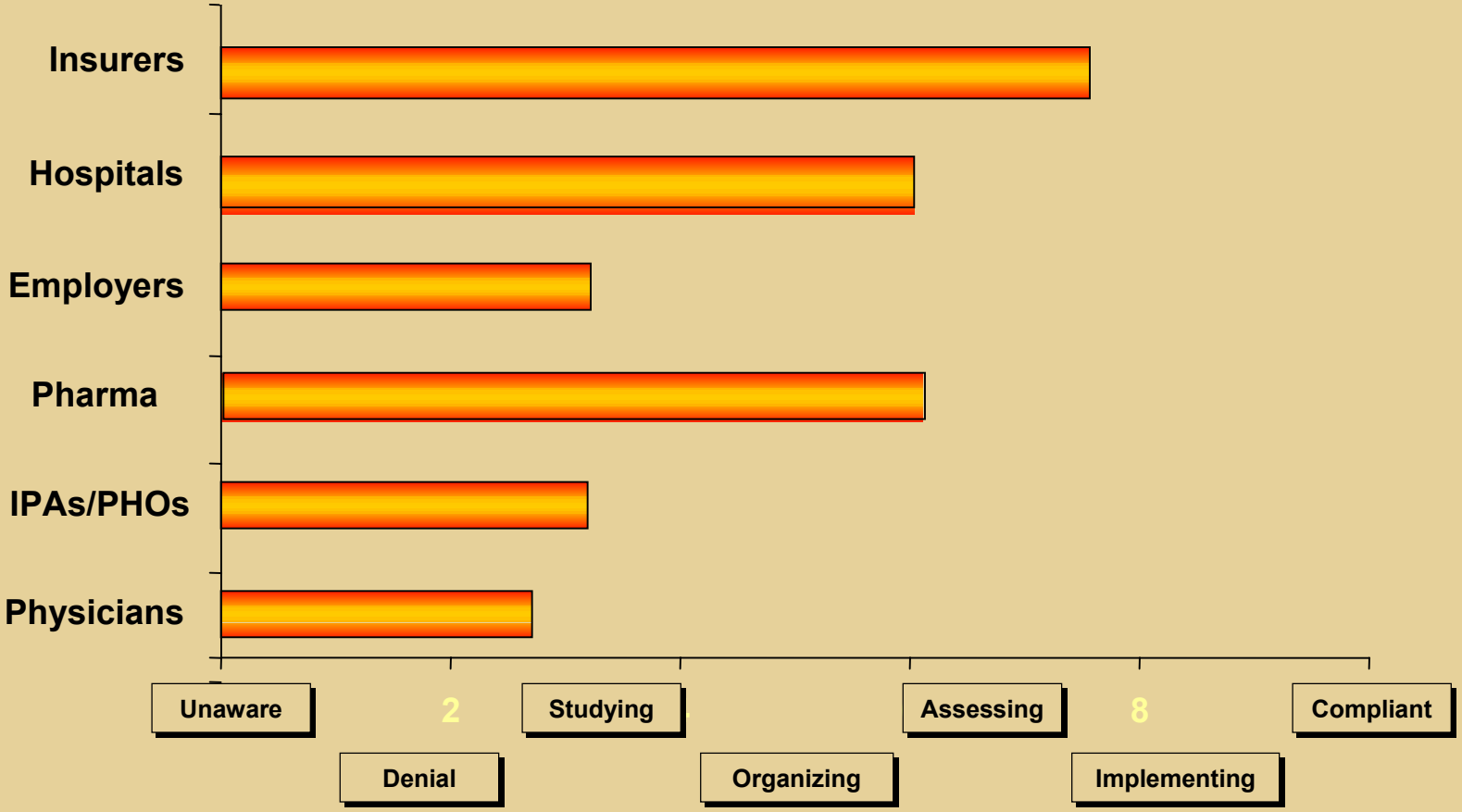
*Transmitting health information electronically for standard transactions

HIPAA Regulatory Timeframe



HIPAA Preparations

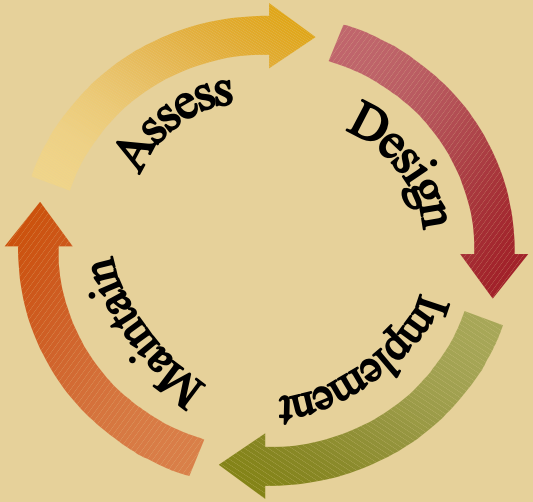
What Others Are Doing...



Security Standards

P w C

Security Standards



Security Life Cycle

HIPAA Security Standard Concepts:

- Comprehensive
- Technology-neutral
- Scalable

Four Categories of Security Requirements:

- Administrative procedures
- Physical safeguards
- Technical security services
- Technical security mechanisms

Security Standards

- Applies to any covered entity that electronically maintains or transmits any health information relating to an individual.
- Electronic transmissions include all media, even when the information is physically moved from one location to another using magnetic tape, disk, or compact disc (CD) media.
- Transmissions over the telephone are not included
- Fax transmission are not included -- this conflicts with the privacy regulations and is expected to be clarified
- No distinction made between internal corporate communication and communication external to the corporate entity.

Security Standards

Administrative Procedures

- Certification, personnel security, internal audit procedures, incident response procedures

Physical Safeguards

- Physical access controls, secure work station location and use, security awareness training

Technical Security Services

- Access control, entity and data authentication, authorization control

Technical Security Mechanisms

- Event reporting, integrity controls, message authentication, encryption on open networks

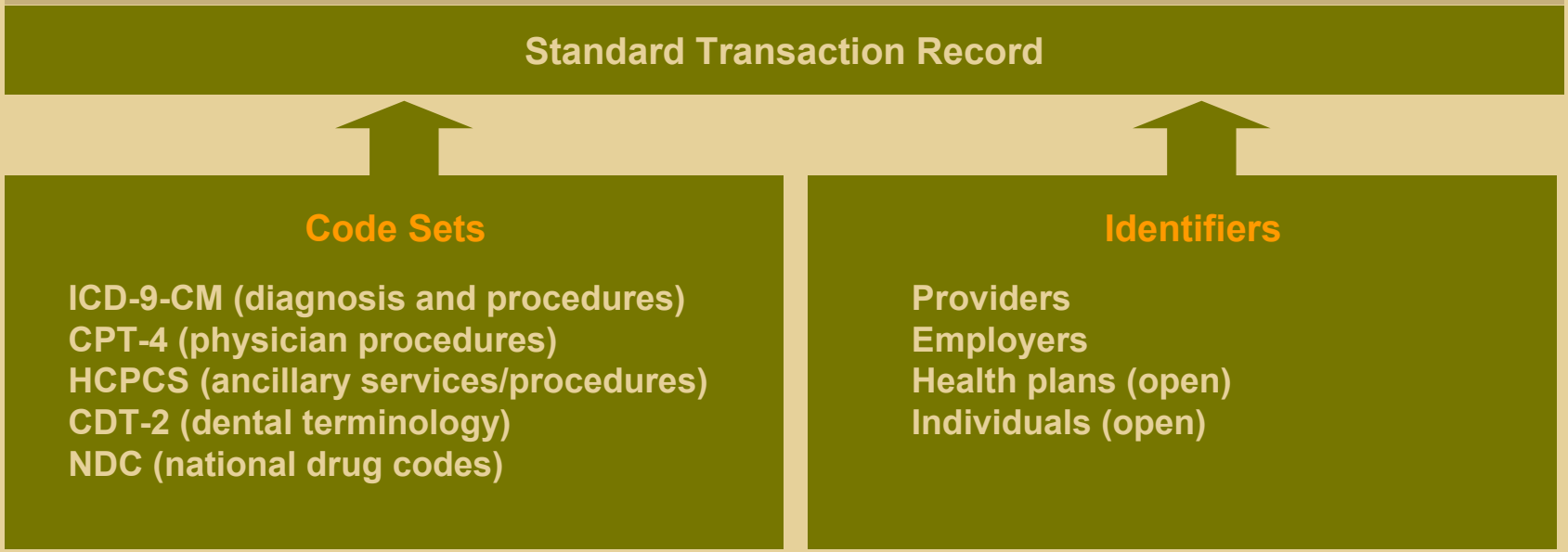
Technology Standards

P w C

Technology Standards

Standard transaction sets are defined for the following:

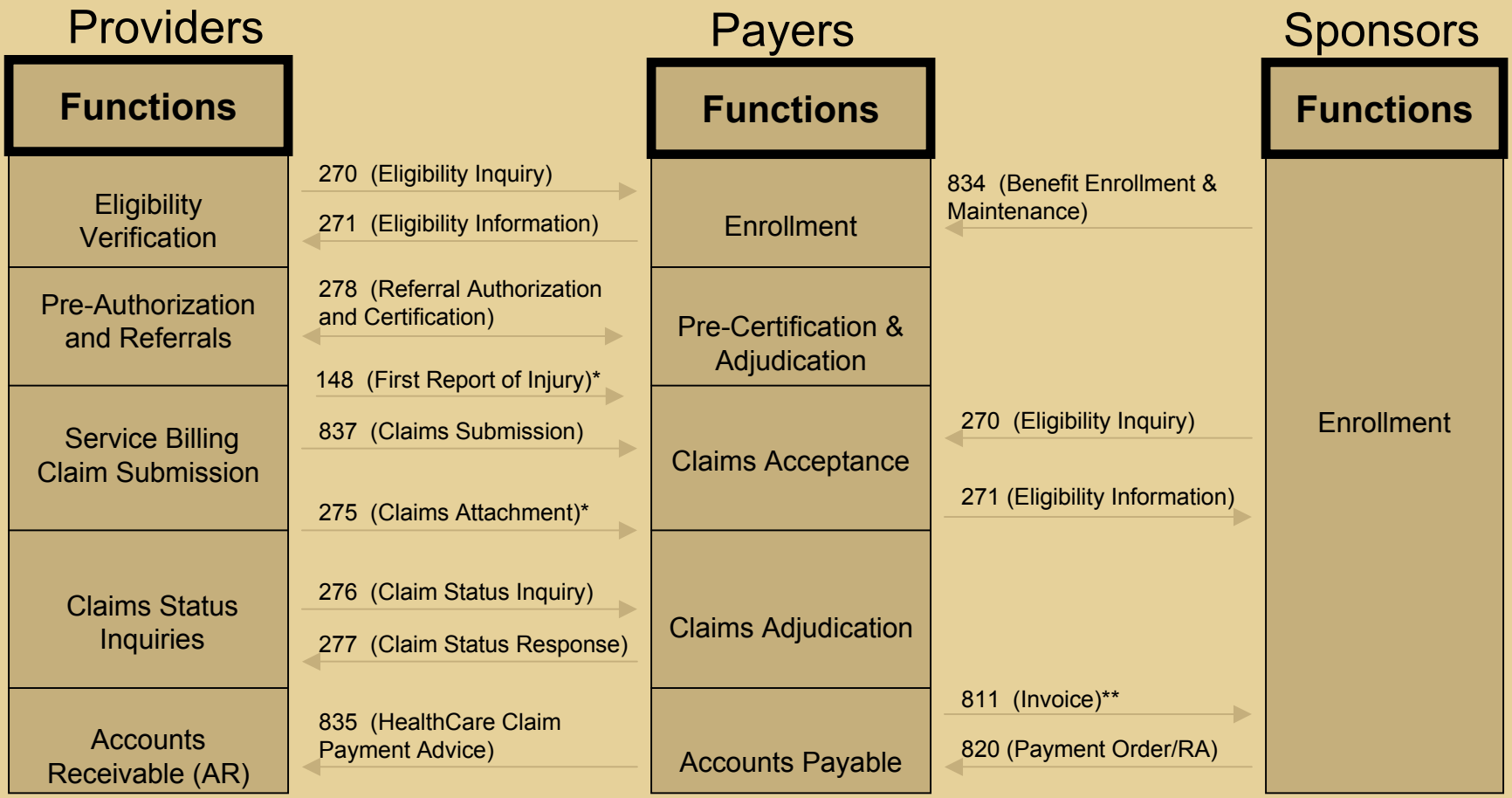
- Health claims or equivalent encounter (X12N 837)
- Retail pharmacy claims (NCPDP Version 5.1)
- Enrollment and disenrollment in a health plan (X12 834)
- Eligibility for health plan - inquiry/response (X12N 270-271)
- Healthcare payment and remittance advice (X12N 835)
- Health claim status - inquiry/response (X12N 276-277)
- Coordination of benefits (X12N 837)
- Referral certification (X12N 278)
- Referral authorization (X12N 278)
- Health plan premiums (X12 820)
- First report of injury (Not in Final)
- Health claims attachments (Not in Final)
- Many Smaller Code Sets



Standard Transactions

- Intended to simplify and enhance electronic data interchange
- Defines “transactions” as the exchange of information between two parties to carry out financial and administrative activities with standard data elements in a single format
- Health plans may not refuse to accept, delay or adversely effect electronic transactions received in standard formats
- Transmissions within a corporate entity would generally have to comply with the standards including the submission of a claim to another health plan
- Covered healthcare entities may use clearinghouses to accept non-standard transactions for translation into the standard transaction formats

Standard Transaction Flows



These are not contained in the initial Transactions and Code Sets Final Rule*

Identifiers

- *Health Care Providers (National Provider Identifier - NPI):*
  - Assigned for life - healthcare provider ID would not change with moves or changes in specialty
  - A single unique identification of an individual provider - must be used in all standard transactions
  - Identifiers must be “intelligence-free” (not contain any encoded information about the healthcare provider)
- *Employers (Employer Identification Number):* Proposed to be current taxpayer identification number used by IRS.
- *Health Plans (Plan ID):* Identifier format yet to be announced; would be assigned to all “health plans”, entities like TPAs.
- *Individual:* Identifier format not yet announced. Very charged issue, vigorously debated and continually delayed.

Privacy Standards

P w C

Privacy Standards

Four Major Categories of Requirements

- Consents and Authorizations
- Minimum Necessary Disclosure
- Rights of Individuals
- Administrative Requirements and Obligations

Relation to State Law

- HIPAA preempts “contrary” provisions of state law unless
- State law provides greater protections or requires higher standard of performance

Penalties

- Administrative penalties / CMPs for minor routine violations
- Criminal penalties and federal prison for major willful or fraudulent violations

Privacy Standards

Individually Identifiable Health Information

- Health information created or maintained by a covered entity or employer that identifies or can be used to identify a specific individual
- Relates to individual's health, health care or payment for care - past, present or future
- Applies to defined standard transactions:
  - provider claims and attachments
  - claim payments and remittance advices
  - premium invoices and payments
  - eligibility information
  - authorization and referral certifications
  - first report of injury

Privacy Standards

Permitted Uses and Disclosures

Treatment, Payment or Healthcare Operations

- For uses / disclosures relating to activities of treatment, payment or health care operations
- Optional consent made at time of enrollment or registration
- Direct providers must give Notice of Privacy Practices, obtain acknowledgement of receipt

Authorization required

- Disclosures on request of individual, the covered entity or a third party
- Disclosure of psychotherapy notes or research information
- Treatment or enrollment/registration cannot be conditioned on provision of authorization
- Marketing communications made using PHI

Privacy Standards

Permitted Uses and Disclosures

- Authorization not required
  - Uses and disclosures required by law
  - Public health, health oversight and regulatory agency activities
  - Cases of neglect, abuse or domestic violence
  - Judicial and administrative proceedings
  - Law enforcement investigations
  - Deceased individuals and organ donors
  - Research purposes (only if waived, then subject to rigorous criteria)
  - Serious threats to health or safety
  - Workers' compensation
  - Disclosure of "de-identified" health information

Privacy Standards

Permitted Uses and Disclosures

- With an opportunity to agree or object, where possible
  - limited information for use in facility directories
  - limited disclosure to family members for follow-up care
  - disaster relief services
  - disclosure to law enforcement regarding victim of a crime
- Fundraising without authorization
  - information on individual demographics or dates of service
  - disclosure to those business associates or institutionally related foundation that assist in the fund raising effort
  - must permit individual to “opt out” from future communications

Privacy Standards

Permitted Uses and Disclosures

- Marketing activities requiring authorization
  - Use PHI to make a “communication about a product or service that encourages recipients of the communication to purchase or use the product or service.”
  - Provision of PHI to another entity for its marketing activities requires that authorization disclose any financial remuneration
- Some “marketing-like” activities do not require authorization
  - face to face encounters or products or services of nominal value
  - health-related products or services of covered entity
  - information on networks, benefits, alternative therapies

Privacy Standards

Minimum Necessary Disclosure (MND)

- Reasonable efforts not to use or disclose more than the minimum amount of information needed to accomplish intended purpose
- For routine uses, MND is determined categorically based on standard protocols and job functions
- For other uses, MND determined on individual basis using criteria
- Related issues
  - Requesting covered entity establishes level of MND in disclosure request
  - MND does not apply for disclosure to a provider for treatment

Privacy Standards

Business Associates

- Contractors assisting or performing functions for covered entities
- Business associate contracts must contain specific privacy provisions
  - Permitted uses and disclosures of PHI
  - Appropriate safeguards of records
  - Report any unauthorized disclosures to entity
  - PHI available for inspection, amendment, accounting
  - Books and records available for inspection by DHHS
  - Destroy/return PHI at termination of contract
  - Material breach by associate is grounds for termination
- Covered entity liable for acts of business associate if it knew of

Privacy Standards

Individual Control of PHI

- Individuals over-age 18 control their health information
  - spouses
  - over-age dependents
- Information of minors is controlled by parents, except:
  - emancipated minors
  - cases where minor receives treatment for a condition for which parental consent is not required by law
  - parental access to minor's PHI determined by state law

Privacy Standards

Rights of Individuals

- Uses and disclosures
  - some permitted only with authorization, some with opportunity to object
  - uses and disclosures for treatment, payment and healthcare operations not subject to authorization
- Request restriction of uses and disclosures (all covered entities)
  - for purposes of treatment, payment or healthcare operations
  - covered entity must honor restriction for six years, if accepted
  - acceptance of request not required

Privacy Standards

Rights of Individuals

- Request restriction on communications
  - by “alternative means” or at “alternative locations”
  - providers must accommodate if reasonable.
  - health plans must accommodate if disclosure could endanger the individual.
- Access to health information
  - for inspection and copying of records as long as entity maintains information
  - covered entity must allow access within 30 days with an extension for off-site records
  - covered entity can charge reasonable fee

Privacy Standards

Rights of Individuals

- Amendment of health information
  - if individual believes records are in error
  - covered entity must evaluate, amend within 60 days if substantiated; one 30-day extension permitted
  - may deny request if not in error or covered entity did not originate
  - must distribute amendment to recipients of erroneous information
- Accounting for disclosures of health information
  - detail of disclosures requiring authorization within past six years with a grandfather clause
  - date, recipient, address, purpose of disclosure
  - one free accounting per year
  - provide accounting within 60 days; one 30-day extension permitted

Privacy Standards

Administrative Requirements

- Designate privacy official
  - Develop privacy policies, administer program
- Designate contact person for privacy complaints
  - Receive and respond to complaints, administer process
- Conduct privacy training program
  - Compliance training for all workers with access to health information
  - Focus on privacy policies and procedures of covered entity
  - Document completion of training and adherence to policies
  - Sanctions for non-compliant staff

Privacy Standards

Administrative Requirements

- Verification procedures
  - Verify identities of individuals requesting individual health information
- Maintain policies and procedures for protection of health information
  - Uses and disclosures
  - Determination of minimum necessary disclosure
  - Monitoring of business associate compliance (implied)
  - De-identification of health information
- Notice of privacy practices
  - Informs patients and/or enrollees of health information practices;

Pharma Potential Areas of Impact

- Drug Discovery
- Research
- Marketing
- Sales
- HR
- Customer Support/Service

Specific Areas of Impact

Discovery

- Genomics/Science
- Gene Studies
- Tissue Samples

Research

- Clinical Trails – phases 1 thru 4
- Use of CROs
- Pharmacovigilance
- Patient Registries
- Financial interests

Specific Areas of Impact

Marketing

- Data Warehouses
- Web Sites
- Direct Mail
- Patient Support Programs
- Disease Management
- Wellness Programs
- Drug Compliance

Sales

- Detail Reps – calling on physicians, preceptorships, etc
- Patient Care Coordinators
- Sales Info (NDC or IMS)
- Switch Programs

Specific Areas of Impact

HR

- Likely covered entity status under HIPAA
- Health Benefits
- Clinics
- EAPs
- Flexible Spending
- Background Checks

Customer Services/Support

- Reimbursement Programs
- Indigent Care/PAP programs
- AE

Questions and Discussion

Brent Saunders
Partner
(973) 236-4682 brenton.saunders@us.pwcglobal.,com

Download PwC's ***Guide to the HIPAA Final Privacy Regulations***
Visit our web site at www.pwchealth.com

P w C