HIPAA Basics:
An Overview of HIPAA Privacy

Rhys W. Jones, MPH
PricewaterhouseCoopers

(813)222-6237
rhys.w.jones@us.pwcglobal.com

www.pwchealth.com

Rebecca L. Williams, RN, JD
Davis Wright Tremaine LLP

(206) 628-7769
beckywilliams@dwt.com

www.dwt.com

PwC

Davis Wright Tremaine LLP

Overview of Privacy

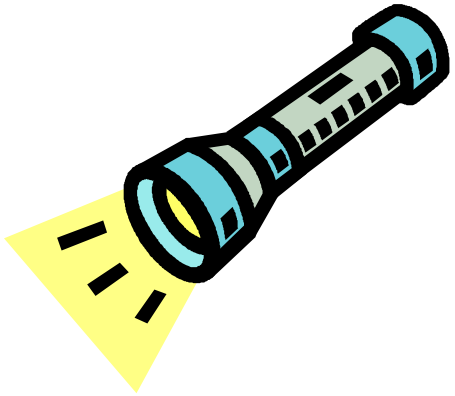
- Privacy is a national topic
- Regular media reports of privacy breaches — particularly electronic information
  - The fear — a couple of clicks can transmit private information all over the world
- Privacy protections exist through —
  - Federal, state and local law
  - Contractual obligations
  - Accreditation standards
  - Ethical considerations
  - Industry custom and practice

Privacy/Confidentiality Laws — Examples

- Substance abuse, mental health and AIDS confidentiality laws
- Privacy Act of 1974
- Consumer protection laws
- Fair Credit Reporting Act
- Children's Online Privacy Protection Act
- Gramm-Leach-Bliley
  - Broad definition of financial institutions
  - Requires disclosure, notice and opt-out provisions
  - Insurers, health plans regulated through NAIC model regs

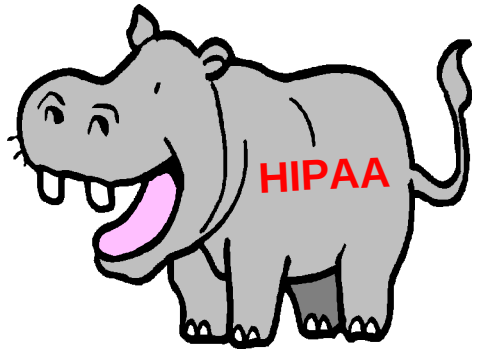
Tort Law — Rights of Privacy

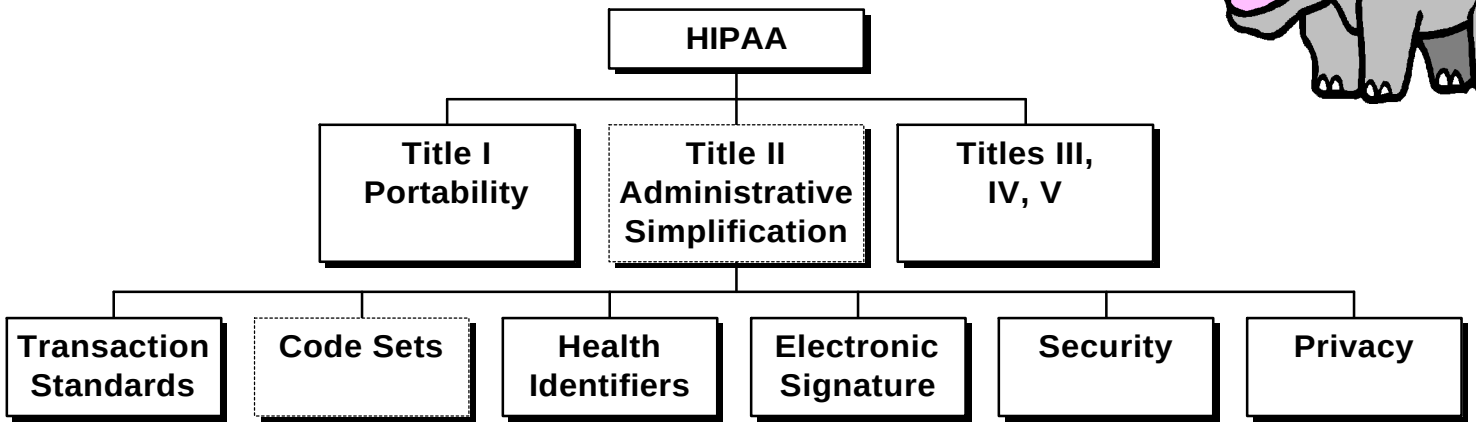
- Privacy rights: Right to be free from —
  - Public disclosure of embarrassing private facts
  - Casting "false light"
  - Misappropriation of name or likeness
  - Intrusion on seclusion or solitude
- Right of publicity
  - Control own name, voice, background and persona for commercial use
- Will HIPAA raise the bar on the industry's standard of care?



HIPAA — Not Just One Issue

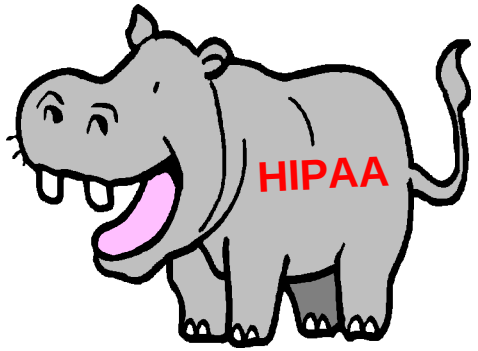
HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996





HIPAA Privacy — Overview

- In promoting EDI and standardization in health care, government recognized need for security and privacy
- Nationalize certain privacy requirements
- Components
  - Enforcement
  - Who and what is covered
  - Use and disclosure rules
  - Individual rights
  - Administrative requirements



A Brief History of HIPAA Privacy

- November 3, 1999 - proposed privacy regulations
- February 17, 2000 - comment period closed
- Record-breaking number of comments received - 53,000!
- December 20, 2000 - final regulations issued
- December 28, 2000 - published in *Federal Register*
- February 28, 2003 - compliance date?
- (small health plans have an extra year)

HIPAA Penalties

- Civil penalties
  - $100 per violation
  - Annual cap: Total penalties not to exceed $25,000 per year for all violations of a single requirement or prohibition
- Criminal penalties
  - Wrongful disclosure — up to $5,000 and/or 1 year jail time
  - False pretenses — up to $100,000 and/or 5 yrs imprisonment
  - For profit/with malice — up to $250,000 and/or 10 yrs in jail
- Other “penalties” or liability
  - Private lawsuits
  - Public opinion/reputation risk
  - Competitive market position

HIPAA Enforcement

- Office of Civil Rights (DHHS)
  - Receive and investigate complaints
  - Compliance review
- Other “interested” agencies
  - FBI, DOJ, OIG
- Covered entities
  - Provide records and compliance report
  - Cooperate with investigations and reviews
- Enforcement regulations
  - coming later this year?

Who Is Subject to HIPAA?

- Covered Entities (direct)
  - Health plans
  - Health care clearinghouses (process nonstandard data elements into standard data elements)
  - Health care providers who electronically transmit any health information in a HIPAA-covered "transaction"

- Business Associates (contractual)
  - Receive PHI from covered entity
  - Perform a function on its behalf
- "Health plan" does not include:
  - Workers' compensation, disability, sickness fund, liability coverage

Who Is Subject to HIPAA?
Special Covered Entities Rules

- Hybrid Entities
  - Single legal entity that is a covered entity
  - Covered functions are not its primary functions
  - Firewall — disclosure to other components must meet requirements
- Multi-Function Entities
  - Combination of provider, plan and clearinghouse operations
  - A component may not share protected information with other components

Who Is Subject to HIPAA?
Special Covered Entities Rules

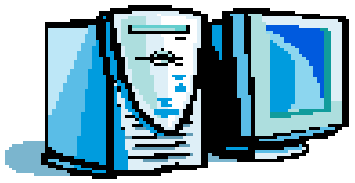
- Affiliated Covered Entities
  - Legally separate covered entities with common ownership and control
  - May designate themselves as a single covered entity
  - Component rules apply
- Organized Health Care Arrangement
  - Separate covered entities
  - Establish clinically and operationally integrated systems
  - Permitted to share information for treatment, management and operations
  - May use common notice and consent

Who Is Subject to HIPAA?
Special Covered Entities Rules

- *Planning consideration:*
  - Covered entity? Hybrid? Multi-function?
  - Generally, separate legal entities have separate obligations
  - Analysis can be complex in multi-entity health systems
  - Determination of HIPAA status is critical up front

What Information Is Covered? Protected Health Information

- Any health information relating to —
  - Past, present or future physical or mental health or condition
  - Provision of health care or
  - Past, present or future payment for health care
- Created/received by provider, plan, employer or clearinghouse
- Individually identifiable or presents reasonable basis to believe the information can be used to identify the individual
- In any medium
  - Written
  - Verbal
  - Electronic



Preemption of State Law

- HIPAA preempts or supercedes all "contrary" state laws
- Exceptions:
  - HHS determination that State law accomplishes social responsibilities (fraud & abuse, industry oversight, health & safety)
  - Public health reporting
  - State law that is "more stringent" —
    - More restrictive use/disclosure rules
    - Greater rights to individuals
- HIPAA — national floor for privacy requirements
- *Planning consideration:*
  - Different privacy environment in each state

Use and Disclosure — General Rule

- A covered entity may not use or disclose protected health information, except —
  - With individual "permission"
    - Pursuant to a "consent" (unless exception applies)
    - As "authorized"
    - After opportunity to agree/object
  - To the individual
  - As otherwise permitted or required under the privacy regulations

Use and Disclosure — Individual "Permission"

Type	*Situation*	*Requirements*
Consent	For treatment, payment and operations	Obtained by provider with direct treatment relationship May be conditioned on care (except emergencies)
Opportunity to Agree/Object	Directory available upon inquiry Clergy inquiry Others involved in care Notification	Verbal → okay Then document
Authorization	Everything else	Written Specific elements No conditioning treatment Revocable

Use and Disclosure — Consent for Treatment, Payment or Operations

- Individual's "consent," prior to use or disclosure, for treatment, payment or health care operations
- Required for providers, optional for payers
- Exceptions:
  - Emergency treatment situations (beware EMTALA)
  - Care required by law but unable to obtain consent (after attempt)
  - Providers with "indirect relationship" to patient
  - Inmates of correctional facilities
  - Substantial communication barriers with inferred consent
- May condition treatment/enrollment on consent

Use and Disclosure — General Consent Requirements

- Content
  - Use and disclose for treatment, payment and operations
  - Refer to notice of privacy practices
  - Reserve right to change privacy practice — state terms and how to obtain revised notice
  - Rights to request limitations or revoke consent
  - Signed and dated by individual
- Must document failure to obtain consent and reasons
- Defective consent = no consent
- Can combine with other consents - separate section and signature
- Joint consents for organized health care arrangement

Use and Disclosure — Opportunity for Individual to Agree/Object

- Verbal request/verbal agreement or objection acceptable
- Situations
  - Directories (with clergy receiving religious affiliation)
  - Persons involved in individual's care
  - Notification
- Allows use of professional judgment and experience with common practice to determine individual's best interests

Use and Disclosure — Individual Authorization

- If not otherwise permitted, must obtain individual's "authorization" for use or disclosure
- May NOT condition treatment on authorization (except clinical trials)
- Given for specific period of time
- Revocable
- Plain language
- "Individual" may be a minor in some cases
- Defective authorization is not valid

Use and Disclosure — Individual Authorization

- Required elements —
  - Meaningful and specific description of information
  - Persons authorized to disclose
  - Persons to whom disclosure may be made
  - Right to revoke
  - Information subject to redisclosure
  - Signature and date
  - Expiration date
- Additional requirements if covered entity requests authorization

Use and Disclosure — Mandatory Disclosure

- To individual upon individual's request
  - Some exceptions apply
- To HHS in connection with its enforcement and compliance review actions
- As otherwise required by law

Permissible Uses and Disclosures Without Patient Authorization

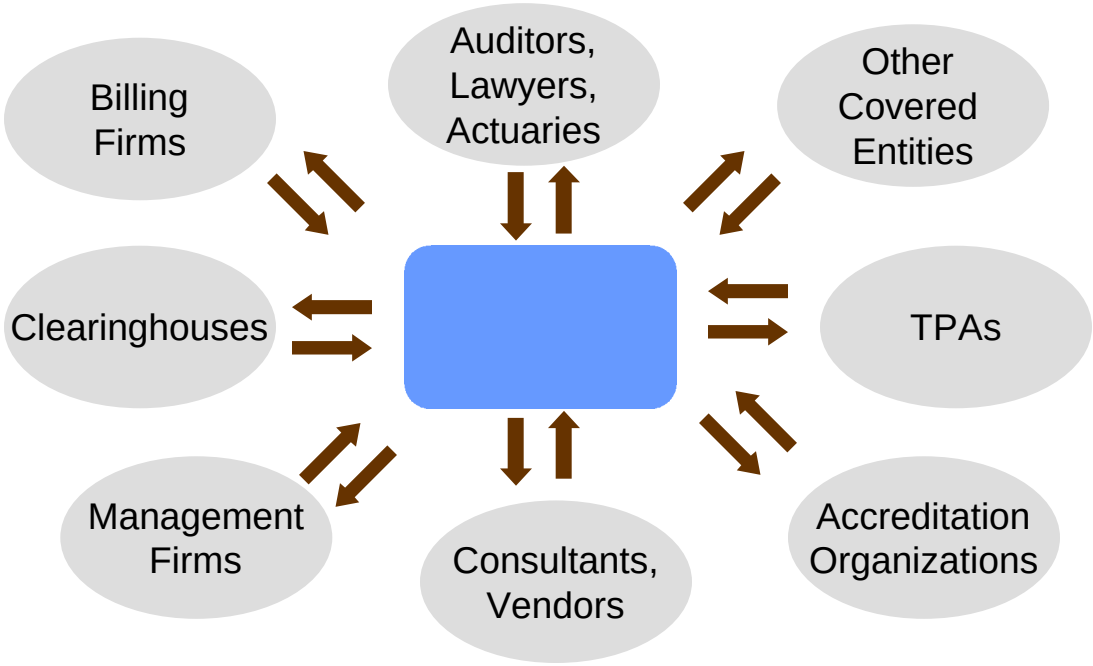
- Public health
- Reporting abuse, neglect or domestic violence
- Health oversight activities
- Judicial and administrative proceedings
- Law enforcement
- Decedents (coroners and funeral directors)
- Cadaveric organ, eye or tissue donation
- Certain research
- Emergency circumstances — avert serious threat to health and safety
- Special categories (e.g. military, VA, intelligence, Department of State)

Use and Disclosure — Marketing and Fundraising

- Marketing without authorization permitted for:
  - Face-to-face encounters
  - Products or services of nominal value
  - Health-related products or services
    - Identify covered entity and whether remuneration was/will be received
    - Ability to opt-out (except widely distributed communications)
- Fundraising without authorization
  - May use or disclose demographic info and dates of service
  - Ability to opt-out
- *Planning consideration:*
  - Careful analysis required for “grey-area” situations

Use and Disclosure — What is a Business Associate?

- A person who, on behalf of a covered entity —
  - Performs or assists with a function or activity involving
    - Individually identifiable information, or
    - Otherwise covered by HIPAA
  - Performs certain identified services



Use and Disclosure — Business Associates

- A covered entity may disclose to business associates if it —
  - Obtains satisfactory assurance that business associates will appropriately safeguard the information
- "Assurance" received through business associate contracts between business associates and covered entity
- If covered entity knows of a pattern of activity constituting a breach by the business associate, then
  - Must take reasonable steps to cure
  - If unsuccessful, must terminate if feasible or report to DHHS
  - Otherwise, considered violation by covered entity

Business Associate Contracts — Required Provisions

- Comply with permitted uses or disclosures
- No further use or disclosure
- Implement appropriate privacy and security safeguards
- Report unauthorized disclosures to covered entity
- Make protected health information available in accordance with individual rights
- Make its records available to HHS for determination of covered entity's compliance
- Return or destroy all protected health information upon termination of arrangement, if feasible
- Ensure its subcontractors comply with same restrictions

Business Associate Contracts — Required Provisions

- *Planning considerations:*
  - Combine business associate and “chain-of-trust partner” agreement required by transaction regulations
  - Addendum vs. separate agreement?
  - Scope - minimum requirements vs. comprehensive agreement?
  - Recontracting logistics - identification, circulation, execution, collection
  - Proactive approach brings competitive advantage?

Minimum Necessary Disclosure

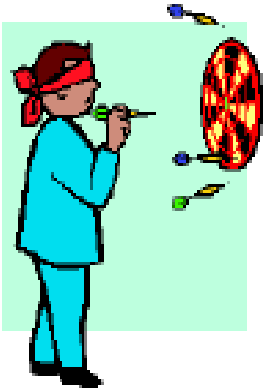
- Amount of information disclosed is restricted to the minimum amount necessary
  - Must make “reasonable efforts” not to use, disclose or receive
  - Minimum amount necessary to accomplish intended purpose
- Identify workforce needing access
- Policies and procedures for recurring and routine disclosures
- Otherwise, determination made on individual basis using covered entity’s criteria

Minimum Necessary Disclosure

- Exceptions:
  - Disclosure to a provider for treatment
  - Release authorized by or for individual's own review
  - Disclosure to HHS
  - Compliance with HIPAA requirements
  - Required by law
- *Planning considerations:*
  - IT reports, user screens
  - Phone and fax disclosures
  - Inter-departmental uses

Use and Disclosure Exception — De-identification

- Use and disclosure restrictions do not apply to de-identified information
  - Does not identify an individual (and no key to re-identify may be disclosed)
  - No reason to believe recipient could identify individual alone or in combination with other information
- Removal of all specific identifiers (18), such as
  - Names of person, relatives, employers
  - Address, phone number, fax, email
  - Social security plan, account, record number
- Determination by statistician that identification is unlikely



Individual Rights — Right to Notice of Privacy Practices

- Written in plain language (with examples in some cases)
- Sufficient detail to put the patient on notice of practices
- Specific content requirements, including —
  - Individual rights to access, inspection, accounting
  - Duties of covered entity
  - Complaints and contacts
- Cannot remove rights through notice
- *Planning considerations:*
  - Reserve right to change notice
  - Changes in notice requires wide scale distribution
  - Anticipate future information needs, include in notice

Individual Rights — Right to Access and Amend

- Right to access own protected health information
  - Reviewable and unreviewable grounds for denial
  - Accepting/denying amendment
  - Rebuttal
  - Documentation
- Right to amend
  - Accepting amendment
    - Amend, distribute to prior recipients
  - Denying amendment
    - Denial letter, statement of disagreement, rebuttal
  - Grounds for denial include
    - Not created by covered entity
    - Disputed PHI is accurate and complete

Individual Rights — Right to Request Additional Protections

- Right to request restriction of further disclosures
  - Covered entity may refuse
  - If agrees → bound (except in emergency)
- Right to request to receive communications in alternative fashion
  - Correspondence sent to alternate address
  - Alternative means of communication
  - Must accommodate reasonable requests

Individual Rights — Accounting of Disclosures

- Right to receive an accounting of disclosures:
  - Date and purpose of disclosure
  - Recipient name and address
  - Description of information disclosed
  - Copies of all disclosure requests
- Exceptions:
  - Treatment, payment and health care operations
  - Health oversight or law enforcement agencies (sometimes)
- *Planning considerations:*
  - Central database to record disclosures by different departments?

Administrative Requirements

- *DOCUMENTED* policies, procedures and systems
- Designate privacy official and contact person
- Implement administrative systems
- Complaint mechanism

- No intimidation/retaliation against individual for exercising rights
- No requirement to waive rights
- Implement administrative, technical and physical safeguards
- Mitigation of harmful effects of improper use or disclosure

Administrative Requirements — Workforce Training and Sanctions

- Privacy and security awareness training
- Training in organization's HIPAA-related policies for:
  - Entire workforce by compliance date
  - New employees following hire
  - Affected employees after material changes in policies
- Documentation of HIPAA training for employees
- Systems of sanctions — consistent enforcement

Summary

- Change in *status quo* - new era of privacy consciousness and protection
- Affects every segment of health care industry, every level of health care organizations
- Very unlike Y2K:
  - Not an IT issue — mostly operational, people processes
  - No endpoint — progresses from planning to implementation to ongoing compliance
- Balancing act:
  - compliance obligations with organizational business objectives
  - process improvement opportunities with implementation costs
- Whether you're ahead or behind, there is still enough time...