

HIPAA Privacy Basics

Presented by:

Michele A. Masucci

Harvey Z. Werblowsky

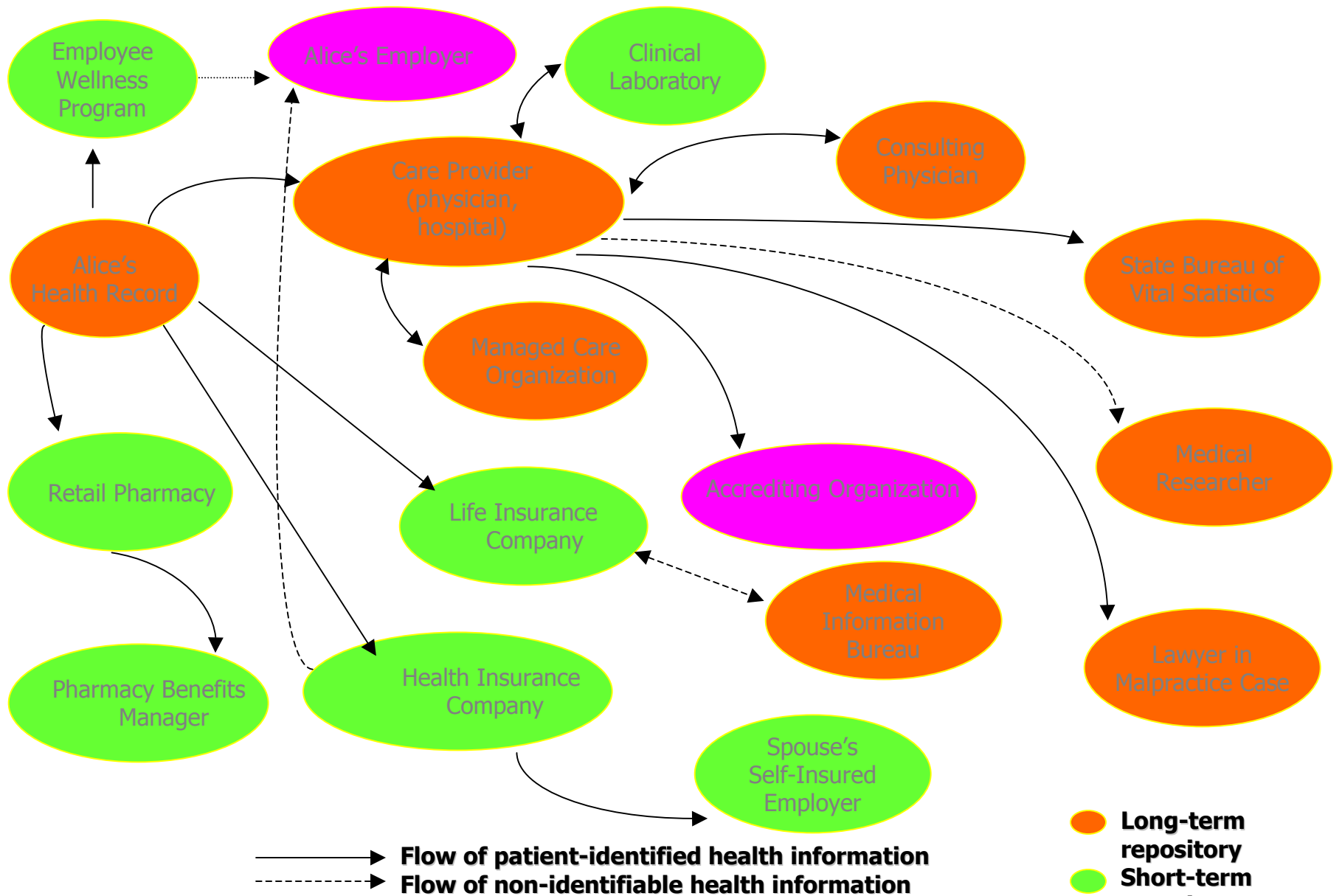
McDermott, Will & Emery

October 30, 2002

Agenda

- Introduction
- Status of Regulations, Acknowledgements, Notice and Authorizations
- Marketing, Business Associates, Minimum Necessary, Research Administrative Requirements,

The Flow of Medical Information



Background

- The Health Insurance Portability and Accountability Act, passed by Congress in 1996
- Goal: Improve the efficiency and effectiveness of electronic information transfers used in the provision, management and financing of health care in the U.S.

Background (cont'd)

- Department of Health and Human Services required to develop rules in four areas:
 - Transactions and code sets [Effective Date extended to October 2003 for those who seek waiver]
 - Identifiers for individuals, employers, plans and providers [on hold]
 - Security standards for administrative, physical, and technical safeguards to ensure data integrity and confidentiality [No regulations yet]
 - Privacy [Effective Date April 14, 2003]

HIPAA REGULATIONS STATUS AS OF SEPTEMBER 2002

HIPAA REGULATION	PROPOSED RULE PUBLICATION	FINAL RULE PUBLICATION	EXPECTED COMPLIANCE DATE
Standards For Electronic Transactions	May 7, 1998	August 17, 2000	October 16, 2002*
National Standard Health Care Provider Identifier	May 7, 1998	Expected 2002	2003
National Standard Employer Identifier	June 16, 1998	Expected 2002	2003
Security and Electronic Signature Standards	August 12, 1998	Expected 2002	2003
Privacy and Patient Confidentiality	November 3, 1999	December 28, 2000	April 14, 2003
Modification to Privacy and Patient Confidentiality	March 27, 2002	August 14, 2002	April 14, 2003
Standards for Electronic Claims Attachments	Expected 2002	Expected 2002	2003
National Standard Health Plan Identifier	Expected 2002	Expected 2002	2003
Enforcement	Expected 2002	Expected 2002	To be effective with each final rule

Status of Privacy Rule

- Effective April 14, 2001
- Compliance mandatory by April 14, 2003
- Office for Civil Rights published guidance to clarify certain issues in July of 2001
- Notice of Proposed Rule Making (NPRM) issued March 27, 2002 proposed certain changes.
- Final Modified Rule published August 14, 2002.

Major Issues

- Applies to all covered entities that transmit PHI in electronic form
- PHI is broadly defined to include oral and written information, not just electronic information
- Very specific procedures regarding Notice of Privacy Practices and Authorizations from patients
- Expansive view of patient's rights, including right to review, suggest amendments, receive a list of disclosures
- Rules are "scalable" to permit flexibility
- Preemption

Basic Requirement

“A covered entity may not use or disclose an individual’s protected health information except as otherwise permitted or required.”

Who is Covered

- Covered Entities:
 - Health Plans
 - Health Care Clearinghouses
 - Health Care Providers who transmit health information in electronic form in connection a transaction covered by HIPAA-claims, payment enrollment, eligibility, etc.

Who Is Covered (cont'd)

- Organized health care arrangements
 - Clinically integrated care settings in which an individual receives care from more than one provider
 - Organized health care systems with multiple covered entities holding themselves out to the public as participating in a joint arrangements and conducting certain joint activities (e.g., QA, UR)



What is Covered

- Protected Health Information
Individually identifiable health information that has been transmitted or maintained in any form or medium (electronic, paper, oral)

What is Covered (cont'd)

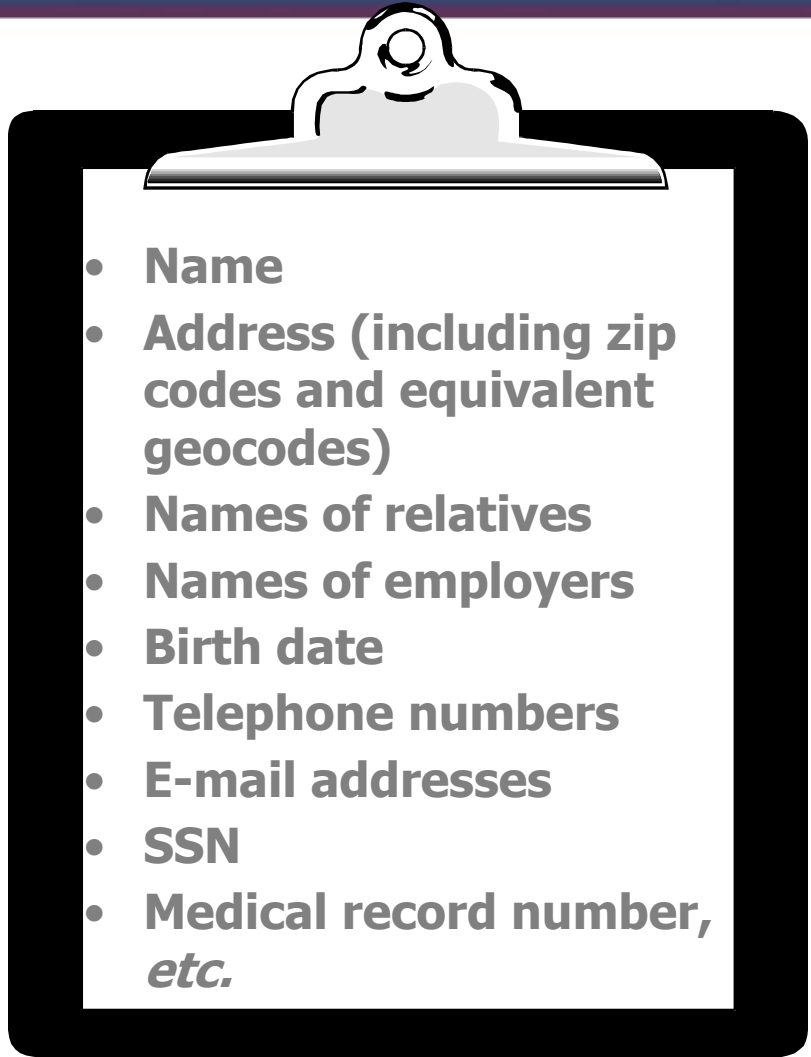
- Individually identifiable health information:
 - Created or received by a provider, plan, employer or clearinghouse
 - Relates to a physical or mental health condition at any time, to the provision of health care or to the past, present or future payment for the provision of health care
 - Identifies the individual or could reasonably be used to identify the individual

The Limitations?

- Except for certain permitted uses or disclosures, Covered Entities cannot *use* or *disclose* protected health information (“PHI”)
 - Goals for compliance:
 - Identify and confirm a permitted use or method of disclosure
- OR
- De-identify the information

De-Identification

- Information is presumed to be “de-identified” if the following has been removed or concealed:

- 
- Name
 - Address (including zip codes and equivalent geocodes)
 - Names of relatives
 - Names of employers
 - Birth date
 - Telephone numbers
 - E-mail addresses
 - SSN
 - Medical record number, *etc.*

Permitted Uses and Disclosures of PHI

- Individual access
- Treatment, Payment, or Health Care Operations (“TPO”)
- By opt-in/opt-out of the subject individual
- As required or permitted by law, e.g., investigations, emergencies

TPO

- CE may use or disclose PHI for its own TPO
- CE may disclose PHI for treatment activities of a health care provider
- CE may disclose PHI to another CE or health care provider for payment activities of the entity that receives the information
- CE may disclose PHI to another CE for health care operations activities of the entity that receives the information, under certain circumstances
- CE in organized health care arrangement may disclose PHI about an individual to another covered entity that participates in the organized health care arrangement

New Requirement for Patient Acknowledgements

- Written Acknowledgement of Receipt of Privacy Notice replaced the consent requirement
- Covered Entity is now required to use “good faith” efforts to obtain the patient’s written acknowledgment of receipt of the Covered Entity’s Notice of Privacy Practices for use or disclosure of patients PHI for TPO
- If acknowledgement cannot be obtained, the Covered Entity must document its “good faith” efforts to obtain the acknowledgement and the reason(s) why it was not obtained¹⁸

General Rules for Optional Patient Consents

- Obtaining consent before using or disclosing the patient's PHI for TPO is now optional
- A Covered Entity which chooses to use written consent has complete discretion in determining the process
- Consent v. Acknowledgement
 - state law
 - prior practice

General Rules for Patient Acknowledgements

- The new modified rule does not prescribe the form or content of the written acknowledgement
- The patient can: (1) initial the Notice, (2) sign a list; or (3) execute a separate document
- “Layered Notice”: short summary of the patients’ rights beneath which is a longer notice that contains all of the elements required by the Privacy Rule and the Modified Rule
- Acknowledgement must be retained by the covered entity in electronic or written form for 6 years

Required Notice of Privacy Practices

- Covered Entities are required to develop Notices of Privacy Practices, Policies and Procedures (describes all permitted uses and disclosures of PHI, individual privacy rights, and privacy policies of provider)
- Post Notice prominently at premises and on websites

Required Notice of Privacy Practices

- Give copy to patient at first service delivery after compliance date
- Obtain patient's Acknowledgement of Receipt of Notice of Privacy Practices
- Make copies available for patients to take
- Produce upon request
- Revise Notice for change in law, policies procedures, practices

Required Notices of Privacy Practices

- Describe Patient Rights to:
 - Restrict
 - Access
 - Amend
 - Accounting
 - Alternative Communication Methods
 - Complain

Timetable for Responses

PATIENT RIGHT

TIMELY RESPONSE

Access

30 days

Amend

60 days

Accounting

60 days



Patient Authorizations

- General Rule for Authorizations - A Covered Entity may not use or disclose PHI for any reason (other than treatment, payment or health care operations) without a valid authorization
- Generally applies to any use/disclosure not for TPO

Patient Authorizations

- Treatment may be conditioned upon receipt of authorization in limited circumstances

Patient Authorizations

Must contain the following core elements:

- description of PHI to be used or disclosed;
- an identification of the persons or class of persons authorized to make the requested use or disclosure;
- an identification of the authorized recipients or class of recipients of PHI;
- a description of each purpose of the requested use or disclosure;

Patient Authorizations

- an expiration date or event related to the individual who is the subject of the use or disclosure or the purpose of the use or disclosure;
- the signature of the individual or the individual's authorized personal representative and date; and
- if signed by a personal representative then a description of the representative's authority to act for the individual.

Patient Authorization

- Authorization required for:
 - disclosure of information to an employer for employment decision
 - disclosure of information for eligibility for life insurance

Patient Authorizations

- Information may be subject to redisclosure and not protected by federal privacy regulations
- Right to refuse to authorize
- Whether direct or indirect remuneration to the Covered Entity will result (for marketing)

Patient Authorizations

- Modified Rule made minor changes to authorization requirements.
- Simplified and consolidated the requirements for authorizations.
- Eliminated requirements to account for disclosures made pursuant to an authorization.

Patient Authorizations

Practical Considerations

- Consider requiring an authorization for release of PHI outside four walls of the Covered Entity, even when not required by HIPAA
- Important to keep track of expiration dates or events

Marketing Communications

- Authorization is not required if:
 - Face to face
 - Nominal products/services

Marketing Communications

- Covered Entity must obtain authorization before making any marketing communications
- Excluded from definition of marketing, communications:
 - that describe the entities participating in a health care provider network or health plan network, or describes if products or services all offered by a provider or plan
 - that relate to treatment of the individual
 - for case management or care coordination for individual, or to direct or recommended alternative treatments, therapies, health care providers or setting of care
- No distinction pertaining to written communications for which the Covered Entity receives compensation

Marketing Communications

Authorization must contain statement that marketing is expected to result in remuneration to physician from 3rd party

Business Associates

- General Rule: a Covered Entity may not disclose PHI to a Business Associate without “satisfactory assurance” that the PHI will be appropriately safeguarded
- A “business associate” is a person or entity who performs a function involving the use or disclosure of PHI for or on behalf of a Covered Entity

Business Associate Rules

- Business associates may include:
lawyers, auditors, consultants, third party administrators, billing companies

Business Associate Rules

- Business associate rules do not apply to the following disclosures:
 - By the Covered Entity to a healthcare provider concerning treatment of the individual
 - By the Covered Entity to an employee
 - By the Covered Entity to a vendor that places its employees on the Covered Entity's premises and the Covered Entity treats such employees as members of its workforce the purposes of complying with HIPAA

Business Associate Rules

- Satisfactory assurance requires a written contract with specific provisions
- Agreement must provide that the business associates shall:
 - Only use or disclose PHI as permitted (i) under the agreement and (ii) by Covered Entities under the Final Rule
 - Use “appropriate safeguards” to prevent use or disclosure of PHI except as permitted by the agreement

Business Associate Rules

- A business associate must also agree to:
 - Report any known misuse of PHI to the Covered Entity
 - Impose the same requirements on its subcontractors and agents
 - Make PHI and an accounting of disclosures available to individuals as required by the Privacy Rule
 - Make its internal practices, books and records relating to use and disclosure of PHI available to DHHS

Business Associate Rules

- Agreements with business associates must also provide that:
 - The Covered Entity may terminate the agreement if the Covered Entity determines that the business associate has breached a material term of the agreement
 - Upon termination of the relationship, the business associate will return or destroy all PHI, if feasible (or extend the protections)

The “Brother’s Keeper” Rule

- A material breach by the business associate of its contractual requirements will be considered noncompliance by the Covered Entity, if the Covered Entity:
 - Knew of such breach and
 - Failed to take reasonable steps to cure the breach or terminate the agreement (or report to DHHS if termination is not feasible)



Business Associate Contracts

- Privacy Rule requires a Covered Entity to amend all contracts with BAs to include the required provisions by April 14, 2003
- Modified Rule allows more time (no later than April 14, 2004) to amend contracts with BAs that are in effect before October 15, 2002
- Compliance is required by the first to occur of the amendment/renewal of the contract or April 14, 2004

Business Associate Contracts

- However, the extension of time to include the required contract language does not postpone the April 14, 2003 deadline for the Covered Entity to ensure that its business associates cooperate in:
 - Disclosures to DHHS of PHI held by the BA
 - Satisfying a patient's right to access, amend or receive an accounting of uses and disclosures of PHI held by the BA

Business Associate Contracts

- Practical implications of revised deadlines
 - Covered Entity should obtain some agreement or assurance that the BA will enable the Covered Entity to satisfy the patient rights by April 14, 2003
 - The Covered Entity will need to obtain compliant BA agreements for new, amended or renewed agreements after the effective date of a revised privacy rule
 - Do not delay - identifying all BAs and negotiating all BA contracts will be time consuming

Business Associate Contracts

- The Modified Rule also provides sample business's associate contract provisions. Note: language changed from "model" to "sample".
- Incorporating such provisions does not serve as a safe harbor from government scrutiny. Rather, it should facilitate the process of adding those provisions that are necessary to comply with the business associate standards.

Business Associate Contracts

- Sample contract language should not be used without analysis
 - Includes obligations of Covered Entity
 - Sample language allows BAs to initially determine whether return of PHI upon contract termination is not feasible
 - No exceptions from limitation of liability or exclusion of consequential damages

Action Steps: Business Associates

- Identify all of your business associates
- Create contract addendum
- Include business associate language in new contracts, as applicable

Business Associates

Practical Considerations

- Less than one year left to review and amend contracts for compliance
- Addition of Business Associate contract provisions may require negotiating
- Review insurance coverage exceptions and indemnification provisions

Minimum Information Necessary

- Privacy Rule requires the Covered Entity to make reasonable efforts to limit the use or disclosure of, and requests for PHI to the minimum necessary to accomplish the intended purposes
- Privacy Rule requires to the Covered Entity to develop and implement policies and procedures appropriate to the Practice's business practice and workforce to limit uses, disclosures and requests of PHI to the amount minimum necessary to accomplish the intended purpose
- The Covered Entity must reasonably ensure that it does not request, use or disclose more than the minimum amount of PHI necessary

Minimum Information Necessary

- May not disclose entire medical record, except to providers for treatment
- Minimum necessary does not apply to uses and disclosures to patients pursuant to an authorization (clarified by Modified Rule), for HIPAA Compliance purpose, that are required by law

Minimum Necessary Requirement

- The minimum necessary standard is a reasonableness standard, intended to be flexible to account for the characteristics of the Covered Entity's business and workforce.
 - Facility redesigns and expensive computer upgrades are not specifically required.
- Minimum necessary standard applies to a Covered Entity's treatment, payment and health care operations.
 - Although minimum necessary standard applies, with respect to treatment, the Covered Entity may develop policies and procedures to enable appropriate individuals within the Covered Entity to have access to the Covered Entity's, PHI, including entire medical record.
 - With respect to disclosures, requests, uses payment and health care operations, Department remains concerned that the Covered Entity will disclose entire medical record unnecessarily.

Minimum Information Necessary

Practical Considerations

- Limit access to PHI to those persons who need access to accomplish their jobs - Role based access
- For each person, identify the category (or categories) of PHI to which access is need and conditions appropriate to access
- Make reasonable efforts to limit access: create access code for computerized medical records system; for paper records, medical records staff must monitor access.
- Reasonable Safeguards

Unintended Uses and Disclosures

- Modified Rule adds a new provision which explicitly permits uses and disclosures that occur as a result of an otherwise permitted use or disclosure under the Privacy Rule.
- Incidental use or disclosure is:
 - a secondary use or disclosure that cannot reasonably be prevented
 - is limited in nature
 - occurs as a by-product of an otherwise permitted use or disclosure
- The Covered Entity must implement reasonable safeguards to limit unintended uses and disclosures and must implement the minimum necessary standard requirements

Unintended/Incidental Uses and Disclosures (cont.)

- The following are incidental uses and disclosures (assuming the Covered Entity otherwise complies with Privacy Rule) which are permitted by the Modified Rule:
 - an unauthorized person overhears a confidential communication between providers
 - discussion of lab results with a patient or other provider in a joint treatment room
 - oral coordination of services at a hospital nursing station
 - utilizing sign-in sheets and calling out patient names in waiting room, so long as the information disclosed is appropriately limited

Unintended/Incidental Uses and Disclosures (cont.)

- The following uses and disclosures are not considered permissible as unintended/incidental:
 - an incidental use or disclosure that occurs as a result of a failure to apply reasonable safeguards or the minimum necessary standard
 - for example, a hospital uses a waiting room sign-in sheet to ask a patient's health history.
 - erroneous uses or disclosures that result from mistake or neglect
 - for example, posting a patient's PHI erroneously on provider's website
 - for example, sending PHI to the wrong person by e-mail

Research

Three pathways for disclosing PHI to researchers:

- 1) Authorization;
- 2) Waiver of Authorization from an IRB or Privacy Board; or
- 3) De-identification

Special Issues for Research

- Research v. Health Care Operations
- Covered Entity involved in research must obtain appropriate authorization from subjects
- Covered Entity must obtain authorization for data bank research unless he receives assurance from Privacy Board of waiver

Administrative Requirements

- Designate Privacy Officer
 - HIPAA is scalable so the privacy officer in a small physician practice may be the office manager
- Designate a contact person
 - Responsible for receiving complaints and providing further information about the Covered Entity's privacy practices

Administrative Requirements

- Must train all personnel on policies and procedures required under the rule
 - E.g., Training may be satisfied in a small physician's practice by providing each member of the workforce a copy of the practice's privacy practices
- Must train personnel on an on-going basis
- Must document training

Administrative Requirements

- Safeguards for Privacy-Must have in place administrative, technical and physical safeguards
 - Does not require the following structural or system changes: private rooms, soundproofing of rooms, encryption of telephone systems
- Internal Complaint Process
- Must accept and maintain a record of all complaints and their disposition

Enforcement

- No private right of action
- Final Rules do not allow patients to sue Covered Entities for violations
- Non-compliance with HIPAA might be the basis of patient negligence lawsuits

Liability for Violations

- Civil Liability
 - DHHS may impose fines of \$100 per violation up to \$25,000 per year for negligent violation of a single standard
- Criminal Liability
 - HHS may make a criminal referral of Department of Justice for a “wrongful disclosure” with fines up to \$250,000 and one to ten year imprisonment