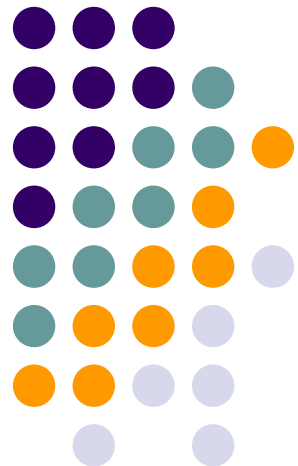
Research Under The HIPAA Privacy Rule

UTHSC Office of Research Compliance, Office of Human Subjects Protection

Lunch & Learn

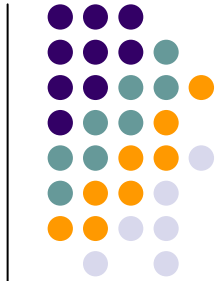
June 11, 2008



Disclaimer

The statutory and regulatory requirements outlined in this presentation are detailed and precise. This presentation is to provide merely an introduction to the subject matter, is for educational and discussion purposes only, and should not be relied on as legal advice or as a complete statement of the law.

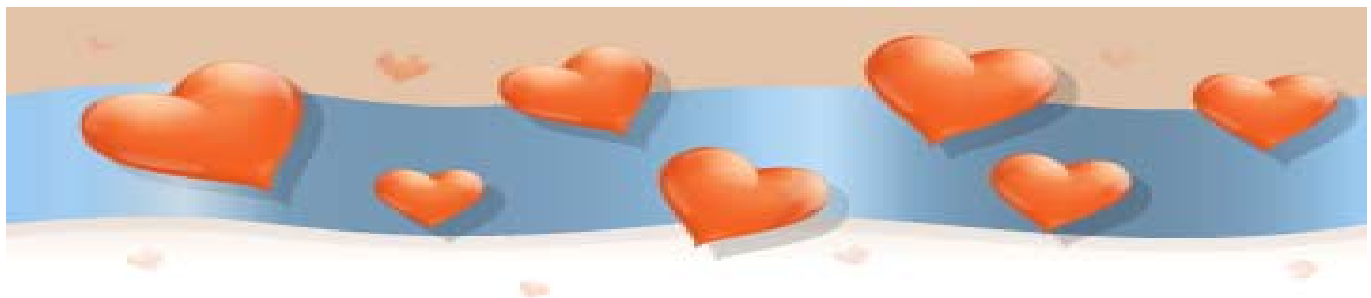
HIPAA Overview



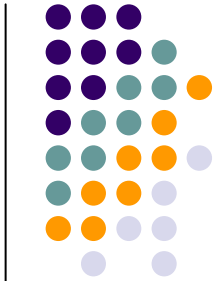
- **HIPAA - Health Insurance Portability & Accountability Act**
  - Passed by Congress in 1996
  - Title I – Protects health insurance coverage for workers and families when they change or lose their jobs
  - Title II – Creates several programs to control fraud and abuse within the health care system
- **Title II - Administrative Simplification**
  - Core Elements:
    - Standardization of electronic data
      - Transaction and Code Set Standards Rule
    - Helping health care organizations better understand what types of information are considered protected
    - Protecting health information transmitted by creating privacy and security requirements

The Privacy Rule

- **Purpose: To provide federal standards for protecting health information**
  - Regulates the use and/or disclosure of an individual's *Protected Health Information*
  - Protects and enhances the rights of individuals by providing certain privacy rights in regard to accessing their health information and by having more control over the use of that information
  - Compliance deadline: April 14, 2003



Protected Health Information (PHI)



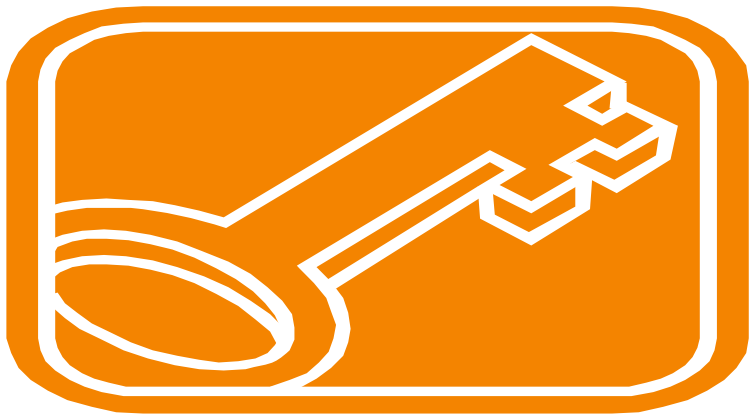
- **Health information must be <u>individually identifiable</u> to be protected by HIPAA**
  - Protected Health Information = *Covered Entity* + Health Information + Identifiers
  - Transmitted or maintained in any form (paper, oral, electronic, forms, web-based, etc.)
  - Exceptions: De-identified health information, Education records covered by FERPA, Employment records held by a Covered Entity in its role as an employer (e.g., FMLA documentation)

What is a Covered Entity?

- **Health care provider**
  - Who transmits any health information electronically in connection with a transaction for which the Secretary has adopted standards
    - Transaction and Code Set Standards Rule
- **Health plan**
- **Health care clearinghouse**
- **Medicare Part D Drug Card Sponsors**
- **Therefore, the Privacy Rule does not apply to All Organizations**
  - Excludes health data held by non-covered entities

Uses and Disclosures

- Use = Sharing, application, utilization, examination or analysis of data containing PHI within a Covered Entity that maintains such data
- Disclosure = Release, transfer, divulging or providing access of PHI to persons or organizations outside the Covered Entity



Routine Permissible Disclosures

(*authorization not required*)

- **Treatment**
  - Provision, coordination or management of health care for an individual by one or more health care providers
- **Payment**
  - Activities of a health care provider to obtain payment or to be reimbursed and activities of a health plan to determine or fulfill responsibilities for coverage
- **Healthcare operations**
  - Examples: Quality assessment and improvement activities; conducting or arranging for medical reviews, audits or legal services; business planning and development

Commonly referred to as "TPO"

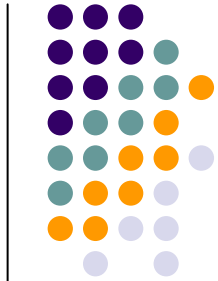
Routine Permissible Disclosures

(authorization not required, but patient given opportunity to object)

- **Facility directory**
- **Individuals involved in care or payment for care**
  - **A Covered Entity may rely on…**
    - An individual's informal permission
      - to disclose to the individual's family, relatives or friends or to other persons whom the individual identifies, Protected Health Information that is
        - directly relevant to that person's involvement in the individual's care or payment of care.

Non-Routine Permissible Disclosures

(*authorization not required*)



- Public health activities
- Victims of child abuse, neglect, domestic violence
- Organ and tissue donation
- Coroners, medical examiners, and funeral directors
- Judicial and administrative proceedings
- Required by law

Required Disclosures

(*authorization not required*)

- **Individual who is the subject of the Protected Health Information**
- **Department of Health and Human Services, for purposes of enforcement and compliance**

Minimum Necessary Standard

- **Use, disclose, or request only the minimum amount of PHI necessary to accomplish the purpose**
- **Exceptions:**
  - Disclosures to or requests by a health care provider for treatment
  - Disclosures made to the patient or to the patient's personal representative
  - Use or disclosure made pursuant to an authorization
  - Disclosures to the Department of Health and Human Services (DHHS) for complaint investigation, compliance review or enforcement

Effects on Research

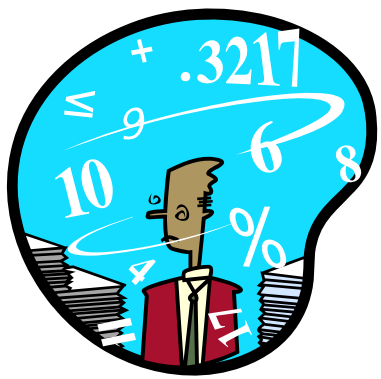
- New Federal rules for disclosing and obtaining health information by Covered Entities
- Creation of Privacy Boards
- Changed informed consent procedures regarding the inclusion of required authorization language
- New rules for tracking release of data
- Created specific penalties (fines and jail time)

Some Things Do Not Change

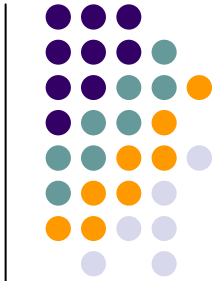
- **Common Rule (HHS Protection of Human Subjects Protection) & FDA Regulations**
  - Privacy Rule enacted in addition to the privacy protections found in the Common Rule and in FDA Regulations
- **State laws still apply, unless HIPAA more stringent**

De-Identified Data Set

- **Health information that has been *de-identified* is not protected by the HIPAA Privacy Rule.**
- **To *de-identify* health information, a researcher must**
  - Remove specific identifiers from the data, or
  - Have the health information de-identified by a statistical expert



Removing Specific Identifiers



- Names
- Geographic information (including city and ZIP)
- Elements of dates (except year), ages over 89 years
- Telephone numbers
- Fax numbers
- Email addresses
- Social Security numbers
- Medical Record or prescription numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- VIN, serial and license plate numbers
- Device identifiers and serial numbers
- Web URLs
- IP address numbers
- Biometric identifiers (finger prints)
- Full face, comparable photo images
- Unique identifying numbers

Allowed in De-identified Data

- Gender
- Specific age under 90
- Grouping for ages over 90
- Codes for re-identifying the data

Common Rule and HIPAA

- Research involving human subjects and PHI is subject to the HIPAA Privacy Rule and the Common Rule
- Higher privacy protection prevails
- IRBs still exist

Research with Individual Permission

- **Common Rule/FDA Regulated → IRB review of research and informed consent**
- **Privacy Rule → Valid authorization**

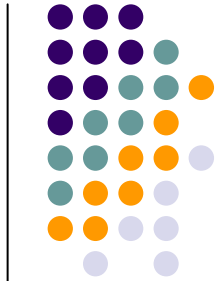
Authorization

- **Written permission from individual**
- **Authorization must be in writing and contain**
  - Certain core elements and
  - Certain statements
  - To be valid
- **A Covered Entity may not disclose PHI if the authorization in question is not valid.**
- **May be combined with Informed Consent when involving participation in research**

Authorization – Core Elements

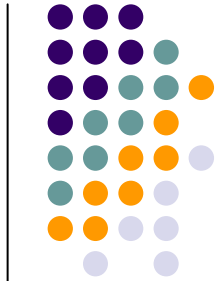
- **Description of information to be used and/or disclosed**
- **Who is authorized to make the disclosure**
- **Who is authorized to receive the information**
- **Purpose**
  - Guidance from HHS regarding scope
- **Expiration date**
  - May be “no expiration date” or may continue “until end of research study”
- **Signature and date**

Authorization – Core Statements



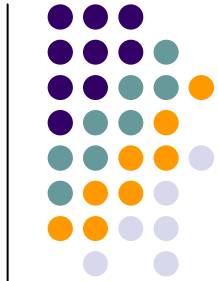
- Right to revoke
- Whether treatment conditioned by authorization
- Risk of future re-disclosure

HIPAA Authorization vs. Informed Consent for Research



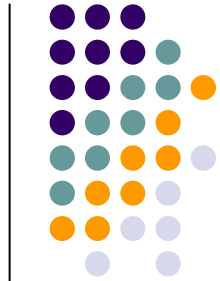
- Authorization focuses on privacy
- Informed consent focuses on risks and/or benefits of study and confidentiality of records
- HIPAA allows combining consent & authorization in one document.

Research without Individual Permission



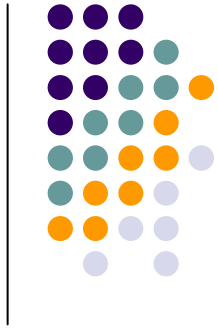
- **Common Rule → IRB Review**
  - Waiver criteria
- **Privacy Rule → IRB/Privacy Board review**
  - Waiver criteria
    - Limited data set, or
    - Preparatory to research, or
    - Research on decedents

IRB Waiver of Authorization Requirement



- A Covered Entity is permitted to use or disclose PHI for research when it obtains or receives documentation of IRB or Privacy Board approval of waiver of Authorization
- IRB established by Common Rule
- Privacy Board established by HIPAA

Criteria for Waiver of Individual Authorization



- **IRB/Privacy Board can grant a waiver of individual authorization if it determines:**
  - Minimal risk to the privacy of individuals because of an adequate plan/assurance
    - Protect identifiers from improper use or disclosure
    - Will destroy identifiers at earliest opportunity consistent with conduct of research
    - Assurance that PHI will not be inappropriately reused or disclosed
  - Research not practicable without access to PHI
  - Research not practicable without waiver

Waiver Documentation – Required Elements

- Name of IRB/Privacy Board
- Date waiver approved
- Description of PHI
- Statement that all specific criteria for waiver met
- Statement of approval
- Signature of IRB/Privacy Board chair

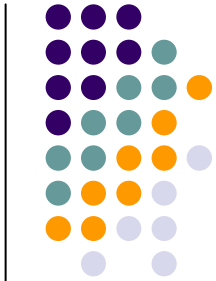
Limited Data Set

- The Privacy Rule permits the disclosure of a limited data set for the purposes of research, public health or health care operations
- Disclosures may not contain direct identifiers
- "Data Use Agreement" required
- Not necessary to obtain patient authorization when this option is used

Data Use Agreement

- **Establishes**
  - Permitted uses and disclosures
  - Identity of recipient
  - Future disclosure or use for other purposes limited
  - Safeguards to protect data
  - Limits on subcontractors
  - Cannot re-identify the data or contact individuals

Limited Data Set Excludes



- Names
- Postal addresses
- Telephone and fax numbers
- Email addresses
- Social Security numbers
- Medical record numbers
- Health plan numbers
- Certificate/license numbers
- Account numbers
- Vehicle ID or license numbers
- Device identifiers, serial numbers
- Web URLs
- Internet protocols
- Biometric identifiers (finger prints)
- Full face photographic images, comparable images

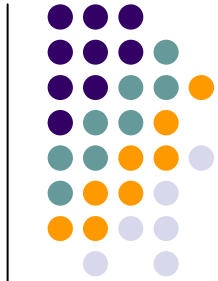
Limited Data Set Allows

- City, state, and 5 digit zip code
- Dates

Preparatory to Research

- **To access health information for preparatory to research activities, the researcher must certify to the Covered Entity that:**
  - The use and/or disclosure is requested solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research, and
  - The PHI will not be removed during the course of the review nor in any way further disclosed in the course of the review, and
  - The PHI is necessary for research purposes.

Preparatory to Research



- **Reviewing charts vs. contacting potential subjects**
  - Researchers, including assistants, who are employees of Covered Entity may contact a potential subject to provide information about a study and to seek authorization.
  - Researchers, including assistants, who are not employees may not use the preparatory to research provision to contact prospective research subjects.
    - Option - Receive and use contact information through a partial waiver of authorization granted by an IRB
    - If not, actual contact must be made by someone who works for the Covered Entity

Research on Decedents

- **Researcher must certify that:**
  - Use and/or disclosure of PHI from records for research involving deceased individuals only
  - The information requested is for research purposes only
- **And, if requested, provide documentation of proof of death (e.g., death certificate)**

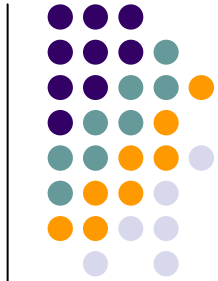
Research Initiated Prior to April 14, 2003

- **Limited grandfather clause**
- **Research allowed to continue if the following was obtained prior to April 14, 2003**
  - Informed consent
  - IRB-approved waiver
  - Authorization or other express legal permission to use or disclose PHI for research
- **Grandfathering ends when any change is made after compliance date makes prior permission invalid.**

Rights of Research Subjects – Access to PHI

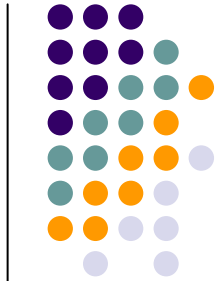
- **With few exceptions, individuals have the right to access, inspect and obtain a copy of information in their designated record for as long as a Covered Entity maintains the information.**
- **However, an individual's access to PHI created or obtained by a Covered Entity/Researcher may be suspended while a clinical trial is in process.**
  - The Covered Entity/Researcher must inform the individual that right to access will be reinstated at the conclusion of the clinical trial.

Rights of Research Subjects – Accounting to Disclosures



- **Individuals have the right to request an Accounting of Disclosures of their PHI**
  - Exclusions:
    - Disclosures for treatment, payment, healthcare operations
    - Disclosures made pursuant to an Authorization
    - Disclosures to individual
    - Disclosures made “incident to”

Rights of Research Subjects – Notice of Privacy Practices



- **Under HIPAA, individuals must receive a Notice of:**
  - A description of the permitted uses and disclosures of their PHI, including for treatment, payment, or health care operations
  - A summary of their privacy rights under HIPAA
  - Legal duties of Covered Entity with respect to PHI

Research Issues for Covered Entities

- **New liabilities for improperly using and disclosing PHI**
- **Review of research protocols**
- **Review of IRB/Privacy Board documentation**
- **Must assess risks and benefits**
- **Agreement preparation**
  - Data use agreement
- **Minimum necessary review**
- **Track and maintain record of PHI disclosures**

Penalties

- **Civil monetary**
  - $100 per violation per person up to a maximum of $25,000 per person per standard violated
  - **Enforced by HHS/Office of Civil Rights**
- **Criminal**
  - Maximum of $250,000, 10 years in prison or both
  - **Enforced by the Department of Justice**

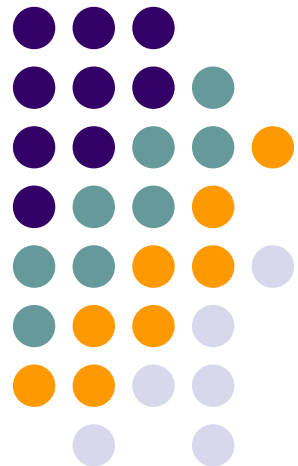
Useful Websites

- **Privacy Rule**
  - http://www.hhs.gov/ocr/hipaa
- **Federal HIPAA Guidelines for Research**
  - http://www.hhs.gov/ocr/hipaa/guidelines/research.pdf
- **National Institutes of Health**
  - http://privacyruleandresearch.nih.gov/default.asp
- **CMS FAQs**
  - http://www.hhs.gov/hipaafaq/permitted/research/index.html

Research Under The HIPAA Privacy Rule

Robert Q. Wilson, Esq.
Partner
The Bogatin Law Firm
(901) 767-1234
rwilson@bogatin.com

Alisa M. Firehock, MHA, FACHE
Privacy Officer and
Director, Office of Clinical Research
UT Medical Group, Inc.
(901) 448-6070
alisa.firehock@utmg.org



Get Hip with

HIPAA

The Health Insurance Portability and Accountability Act